

منشورات اليونسكو

منظمة الأمم المتحدة للتربية والعلم والثقافة

دراسة استقصائية عالمية

حول خصوصية الإنترنت وحرية التعبير

إعداد توبي مندل (Toby Mendel) وأندرو بوديفات (Andrew Puddephatt)
وبن واجنر (Ben Wagner) وديكسي هوتن (Dixie Hawtin) ونتاليا توريس (Natalia Torres)

سلسلة اليونسكو بشأن حرية الإنترنت

دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير

دراسة استقصائية عالمية

حول خصوصية الإنترنت وحرية التعبير

إعداد توبي مندل (Toby Mendel) وأندرو بوديفات (Andrew Puddephatt)
وبن واجنر (Ben Wagner) وديكسي هوتن (Dixie Hawtin) ونتاليا توريس (Natalia Torres)

سلسة اليونسكو بشأن حرية الإنترنت

المؤلفون

- أندرو بوديفان (Andrew Puddephatt)، المدير، جلوبال بارتنزر آند أسوشيتس
- توبي مندل (Toby Mendel)، المدير التنفيذي، مركز القانون والديمقراطية
- بن واجنر (Ben Wagner)، باحث، معهد الجامعة الأوروبية
- ديكسي هوتن (Dixie Hawtin)، مدير مشروع، جلوبال بارتنرز آند أسوشيتس
- نتاليا توريس (Natalia Torres)، باحث، مركز الدراسات المعنية بحرية التعبير والوصول إلى المعلومات (CELE) التابع لجامعة باليرمو، الأرجنتين

ونتقدم بشكر خاص إلى الأشخاص التالين الذين تكرموا بالموافقة على أن نتحاور معهم عند إعداد هذا المنشور:

غاو لينانج (Guo Liang)، يانغ وانغ (Yang Wang)، سيرين أونال (Ceren Unal)، أنغ بينغ هوا (Ang Peng Hwa)، إيريك إيريارت أهون (Erick Iriarte Ahon)، كاتيتزا رودريجيز (Katitza Rodriguez)، كارين ريلي (Karen Reilly)، علي جي رافي (Ali G. Ravi)، معز شاشكوك (Moez Chackchouk)، بريمافيرا دو فيليبي (Primavera de Filippi)، بيتر باريسيك (Peter Parycek)، روبيرت بودل (Robert Bodle)، سمير بادانيا (Sameer Padania)، بيتر برادويل (Peter Bradwell)، أولريك هوبنر (Ulrike Höppner)، إيدواردو بيرتوني (Eduardo Bertoni)، هونغ زيو (Hong Xue)،
مونيك فانجوي (Monique Fanjoy)، أبوبكر منير، جو مكنامي (Joe McNamee)، عمر غربية، جامي هورسلي (Jamie Horsley)، نبيوموسينو مالالوان (Nepomuceno Malaluan)، سينثيا إم ونج (Cynthia M. Wong)، سينفه تونساراووث (Sinfah Tunsarawuth)، بريم أوت فان دالين (Prim Ot van Daalen)، سونيل أبراهام (Sunil Abraham) وعدد لم تذكر أسماؤهم من الموظفين السابقين لدى بعض شركات التكنولوجيا الكبرى.

طبع في 2012 من جانب
منظمة الأمم المتحدة
للتربية والعلم والثقافة (اليونسكو)
7, place de Fontenoy, 75352 Paris 07 SP, France

الترقيم الدولي: ISBN _978_92_3_604241_1

تمت ترجمة وطباعة هذا الكتاب باللغة العربية بفضل مساهمة الوكالة السويدية للتعاون الإنمائي الدولي (سيدا)

قام بالتنسيق والطباعة منظمة اليونسكو

تم طباعة هذا المنشور لأول مرة بفضل مساهمة الوكالة السويدية للتعاون الإنمائي الدولي (SIDA)

طبع في فرنسا

المحتويات

تمهيد

تعمل منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو) ومن منطلق ما نص عليه نظامها الأساسي، على دعم «حرية تدفق الأفكار بالكلمات والصور»، ولقد آلت على نفسها العمل على تمكين فضاء الكتروني حر ومتاح يسهل للجميع الوصول إليه في إطار دعمها لحرية التعبير الشاملة على الإنترنت وخارج الإنترنت.

وكما هو موضح في منشور اليونسكو الصادر عام 2011 بعنوان «حرية التعبير: حرية الاتصال، الإيكولوجيا القانونية والتنظيمية المتغيرة التي تتشكل منها الإنترنت"، إن الحرية ليست نتاجاً ثانوياً تحتم عن التغير التكنولوجي، ولابد من حمايتها باستخدام التدابير القانونية والتنظيمية اللازمة من منطلق إدراكنا التام في هذا العصر الذي يتسارع فيه التغيير بأن حرية التعبير على الإنترنت هي من المسائل المعقدة، بما يستوجب العمل على إيجاد التوازن بين هذا الحق وغيره من المتطلبات الأخرى، المتضاربة أحياناً – مثل الأمن القومي وحماية حقوق المؤلفين واحترام الخصوصية.

وتصدر اليونسكو هذه المسائل في إطار عملية متابعة منتدى القمة العالمية لمجتمع المعلومات (World Summit of Information Society) وأنشطتها المتعلقة بمنتدى إدارة الإنترنت.

ونحن نعلم جيداً أننا أصبحنا نعيش في عالم بلغ مستخدمو الإنترنت فيه حاجز المليارين ووصل عدد مستخدمي الهواتف النقالة فيه إلى خمسة مليارات يقومون جميعاً بنشر ملايين المدونات والتغريدات (tweets) والصور وملفات الصوت والصورة (البودكاست – podcast)، فضلاً عن المعلومات الشخصية كل يوم.

ومن هذا المنطلق، أدركت اليونسكو أن للخصوصية، بوصفها حق من الحقوق الأساسية، تأثيراً على الحقوق والحريات الأخرى، بما فيها حرية التعبير وحرية تكوين الجمعيات وحرية العقيدة. والتحدي الماثل هو أنه يمكن استغلال آليات حماية الخصوصية على الإنترنت في بعض الأحيان للتعدي على حرية التعبير المشروعة بشكل عام والأدوار الديمقراطية للصحافة بشكل خاص. بل هناك تحد آخر عند إيجاد التوازن بين هذه الحقوق على الإنترنت وهو يكمن في تفاوت الشبكات القانونية بين المجتمعات المتصلة بالإنترنت وغير المتصلة بالإنترنت، بالإضافة إلى الولايات القضائية القومية والدولية.

يسعى هذا المنشور، مع أخذ كل هذه الأمور بعين الاعتبار، إلى تحديد العلاقة بين حرية التعبير وخصوصية الإنترنت، وتقييم مواضع دعم بعضها البعض أو تعارضها مع بعضها البعض في ظروف مختلفة. ويوضح المنشور بالتفصيل هذه المسائل في البيئة التنظيمية الحالية لخصوصية الإنترنت من منظور حرية التعبير. فهو يعرض نظرة عامة عن الحماية القانونية والمبادئ الإرشادية ذات التنظيم الذاتي والتحديات المعيارية ودراسات الحالة المتعلقة بالموضوع.

ونأمل أن يكون هذا المنشور أداة مرجعية ذات فائدة لدول أعضاء اليونسكو والمعنيين الآخرين على المستوى القومي والمستوى الدولي بما يقدمه من معلومات حديثة ودقيقة بشأن المسائل الطارئة التي تتعلق بالدول النامية والمتقدمة على حد سواء. حيث يمكن للعديد من المعنيين، وخصوصاً المعنيين بالحوار، استخدام هذا المنشور في نطاق أعمالهم، وأخذ ما يتلاءم معهم من التجارب الواسعة الواردة طي صفحاته التالية. كما يوفر المنشور أيضاً مصادر مرجعية إضافية للقراء المهتمين للاستعانة بها في مزيد من البحث حول الموضوعات محل النقاش.

ونأمل أن يساهم هذا المنشور في جمع المعنيين من أجل المناقشة المستنيرة حول المناهج المؤدية إلى حماية الخصوصية دون المساس بحرية التعبير. وفي السنوات القادمة، سوف تسعى اليونسكو خصيصاً إلى نشر معلومات تتعلق بالممارسات الجيدة والتعاون الدولي بشأن نقاط التداخل بين حرية التعبير والخصوصية. وسوف يظل البحث بشأن حماية مبدأ حرية التعبير في سياسة الإنترنت لمجموعة من المسائل جزءاً من الولاية الطبيعية لليونسكو والاستشارة الفنية التي تقدمها إلى المعنيين.

Jānis Kārkliņš
مدير عام مساعد
قطاع الاتصالات والمعلومات
منظمة الأمم المتحدة للتربية
والعلم والثقافة (اليونسكو)

الملخص التنفيذي

تعد الخصوصية حق من الحقوق الأساسية، وإن كان من الصعب تعريف مضمون هذا الحق على وجه الدقة. ويمكن اعتبار الخصوصية ذات شكل ثنائي – فهي معنية بالمعلومات أو الجانب الذي نحتفظ بخصوصيته في حياتنا؛ ومعنية كذلك بالطريقة التي يتصرف فيها الآخرون بالمعلومات التي لديهم – سواء كانت معلومات محمية أو مشتركة، ومن له الحق في الاطلاع عليها وبأي شروط يجوز معرفتها.

ولقد تشكل فهم الخصوصية بفعل التقنيات منذ فترة بعيدة، حيث عمت بوادر القلق بشأن الخصوصية صفحات المجلات في القرن العشرين. فجاء الإنترنت بدوره ليعيد حتماً تشكيل فهمنا لماهية الخصوصية في العالم المعاصر.

إن الحق في الخصوصية هو أساس الحقوق والحريات الأخرى، بما في ذلك حرية التعبير وحرية تكوين الجمعيات وحرية العقيدة. ولقد لعبت القدرة على التواصل تحت ستار مجهول دون معرفة الحكومة للهوية، على سبيل المثال، دوراً مهماً وتاريخياً في حماية التعبير الحر وتعزيز المسائلة السياسية، مع زيادة احتمالية تعبير الناس عن آرائهم بشأن قضايا تهم المصلحة العامة إن كانت عندهم المقدرة دون أن يخافوا الانتقام. ولكن في ذات الوقت يمكن للحق في الخصوصية أن يتعارض مع الحق في حرية التعبير، ولابد في الواقع من إيجاد توازن بين هذين الحقين. مع العلم بأن إحداث هذا التوازن هو مهمة معقدة، ولا يسهل توقعها سلفاً. ولهذا السبب، ظلت هذه المسألة محل اهتمام المحاكم كي تتمكن من إدارة هذه العلاقة.

يشكل الإنترنت تحديات كبيرة جديدة فيما يتعلق بحماية الحق في الخصوصية. فهو بشكل عام:

- يمكن من جمع أنواع جديدة من المعلومات الشخصية – فقد نتج عن التقدم التكنولوجي ابتكار أدوات لجمع وفهم أنواع مختلفة من المعلومات كان يستحيل أو من غير الممكن الوصول إليها في الماضي.
- يسهل من جمع المعلومات الشخصية وتحديد مواقعها – يختص كل جهاز كمبيوتر أو هاتف نقال أو أي جهاز آخر متصل بالإنترنت بعنوان بروتوكول إنترنت (IP) فريد يوفر محدد هوية فريد لكل جهاز، وهو ما يعني أنه يمكن تتبع هذه الأجهزة. فالقدرة على تحديد موقع أي جهاز من الأجهزة نشأ عنها تحديات كبيرة وجديدة بشأن الخصوصية.
- يهيئ قدرات جديدة للحكومة والقطاع الخاص لتحليل المعلومات الشخصية. فالقوة الحاسوبية الزائدة تعني أنه يمكن بدون تكلفة وبشكل فعال تخزين كميات هائلة من المعلومات ودمجها وتحليلها بمجرد جمعها. ويسمح التقدم التكنولوجي بالربط بين قواعد بيانات المعلومات مع بعضها البعض، الأمر الذي يتيح المزيد والمزيد من كميات البيانات التي يمكن معالجتها.
- يهيئ فرصاً جديدة للاستخدام التجاري للبيانات الشخصية. حيث إن الكثير من الخدمات التي تقدمها هذه الشركات هي خدمات مجانية وتعتمد نماذج أعمالها على جمع معلومات المستخدم واستخدامها في أغراض التسويق.
- ينتج عن تحديات جديدة بشأن التنظيم نظراً لطبيعة الإنترنت العابرة للحدود القومية. وعلى الرغم من ظهور معايير أفضل الممارسات الدولية لجمع البيانات، لا يزال ثمة المزيد من التقدم الواجب إحرازه نحو التقريب بين القوانين القومية. فلا تزال الشركات المتصلة بالإنترنت تواجه صعوبة في تجاوز الشبكة

المعقدة من قوانين الخصوصية القومية عند تنفيذها لخدمات إنترنت دولية عبر الحدود القومية، مع تقويض حماية الخصوصية بسبب الغموض القانوني.

نناقش في القسم 2 من هذا المنشور مجموعة من التهديدات التي تتعرض لها الخصوصية بمزيد من التفصيل والتي تطورت من خلال الإنترنت، ونتطرق في هذا الصدد إلى الأمور التالية:

(1) فرص وتحديات المراقبة المستمرة للبيانات الشخصية على الإنترنت.

(2) مجموعة من المبادرات لحماية الخصوصية وعدم إظهار الهوية على الإنترنت.

(3) أدوار ومسؤوليات مزودي الخدمات والوسطاء.

(4) التحديات المحددة التي تمثلها التطبيقات وبرامج الاتصال ونماذج الأعمال بما في ذلك الحوسبة السحابية ومحركات البحث وشبكات التواصل الاجتماعي وغيرها من الأجهزة المختلفة.

(5) المشاكل التي تنتج عن الحكومة الالكترونية وغيرها من مناهج الإدارة.

(6) التهديدات التي تمثلها الآليات المختلفة للمراقبة وجمع البيانات، ومنها: أدوات تحديد الهوية الفريدة؛ وملفات تعريف الارتباط (Cookies) (وغيرها من الأشكال المرتبطة بتحديد هوية المستخدم)؛ وبرامج الدعاية (Adware) وبرامج التجسس (Spyware) والبرمجيات المؤذية (Malware) التي تسمح بالدخول والمراقبة بالبيانات الخفية؛ وبرامج التفتيش العميق في الحزمات (DPI)؛ ومعالجة البيانات وتكنولوجيا التعرف على الوجه والمراقبة.

ثم ننتقل في القسم 3 إلى المعايير القانونية الدولية المعنية بالخصوصية والردود على هذه المسائل الطارئة، حيث يوضح هذا القسم الفهم والحماية لحق الخصوصية من حيث الظاهر بموجب القانون الدولي لحقوق الإنسان. ثم ينتقل القسم إلى تحليل الأطر التشريعية والتنظيمية الأساسية التي تؤثر على حماية حقوق الخصوصية على الإنترنت على المستويين الإقليمي والقومي في جميع دول العالم؛ ويحلل كذلك نقاط القوة والضعف الكامنة في التنظيم الذاتي لأداة حماية الخصوصية – سواء استخدمت كآلية مركزية أو كانت مكملة للحماية القانونية.

وتتصل حقوق الخصوصية وحرية التعبير ببعضها البعض في صور يكتنفها التعقيد – ونتطرق في القسم 4 إلى هذه التداخلات بمزيد من التفصيل. ففي بعض الأحيان، تكون الخصوصية شرطاً مسبقاً لابد منه لصون حرية التعبير – وبالأخص في الدول التي قد يكون فيها من الخطر تناول قضايا معينة علناً (مثل السياسة والدين والجنس). ولكن ثمة توترات كبيرة بين كل حق من الحقين المذكورين، وذلك مثلاً عندما ترغب صحيفة من الصحف نشر تفاصيل خاصة عن أحد السياسيين البارزين ربما من منطلق اعتقاد الصحيفة أن هذا يخدم المصلحة العامة. ولقد برزت هذه التوترات بروزاً أكبر في ظل التغيرات الهائلة في حرية التعبير التي انبثقت عن الإنترنت وغيرها من أنظمة الاتصال الرقمية.

ونبحث في هذا المنشور في القانون الدولي وممارسات الدول الأخرى فيما يتعلق بصون الخصوصية على الإنترنت، مع الأخذ في الاعتبار التناقضات المحتملة مع الحقوق الأخرى، وبالأخص حرية التعبير. ويحتوي القسم 5 على توصيات نقدمها إلى الدول والشركات من أجل الممارسة الأفضل على أساس البحث والتشاور. وتغطي هذه التوصيات: التدابير القانونية والتنظيمية (التدابير الدستورية، الحماية في القانون المدني والجنائي، أنظمة حماية البيانات) وسياسة وممارسات الشركات وزيادة مستوى الوعي.

وأخيراً، نستعرض في القسم 6 الأبحاث السابقة والمواد والأدوات التي استندنا إليها بشأن السياسة والممارسة الدولية والقومية فيما يتعلق بالخصوصية وحرية التعبير على الإنترنت. ويقصد من هذا القسم أن يكون مصدراً للقراء الراغبين في الرجوع إلى المزيد من الأدوات والوثائق والمعلومات.

1. مقدمة

إن الحاجة إلى الخصوصية هي من الحاجات الراسخة في كيان البشرية، وهي بطبيعتها الأساسية تقوم على مفهوم النزاهة والكرامة الشخصية. ولكن يصعب وضع تعريف دقيق لها يتفق عليه الجميع – فهي في سياقات مختلفة تغطي حرية الفكر والضمير، وحرية الوحدة، وحرية التحكم في الجسد، وحرية حماية السمعة، وحرية الحياة العائلية، وحرية ممارسة الجنس وفق الرغبة الخاصة. وتختلف هذه التعاريف من سياق إلى آخر. وعلى الرغم من وجود الخصوصية في كل مكان، إلا أنه ليس هناك تعريف واحد لها يمكن فهمه بطريقة واحدة على مستوى العالم. وللخصوصية في عالمنا المعاصر بُعدان – الأول تلك المسائل المتعلقة بهوية كل شخص، والثاني طريقة التعامل مع معلوماته الشخصية.

لقد أدت التقنيات المتاحة إلى تبلور طرق الفهم المختلفة للخصوصية، فتضمنت الخصوصية في أكثر المستويات وضوحاً تقييد التعدي على المكان المادي وحماية المسكن والممتلكات الشخصية، ولهذا تركزت سبل حماية الخصوصية في أولى مراحلها على حرمة المسكن والحياة الأسرية. ولكن جاءت تكنولوجيا الاتصالات لتجلب معها مخاوف جديدة تتعلق بمراقبة ما هو معلوم من معلومات عن أي شخص. مع العلم بأن المخاوف المتعلقة بالتعدي على الخصوصية ليست بالأمر الجديد – ففي الواقع، يمكن القول بأنها من سمات القرن العشرين. فقد عرف كل من وارين وبرانديز (Warren & Brandeis) الخصوصية بأنها "الحق في أن يُخلى المرء وشأنه" وذلك في الورقة المواضعية التي أعدت بعنوان "الحق في الخصوصية" في عام 1890 والتي أعدت في وقت كانت تنشر فيه الصحف صور الأشخاص لأول مرة. وجاء هذا التعريف – الذي أفرزته التكنولوجيا الناشئة كما هو الحال بالنسبة للخصوصية دائماً – متعلقاً بحماية "الشخصية المقدسة" وشمول قيم مثل الكرامة الشخصية والاستقلالية الشخصية والاستقلال[1]. وأدى نمو وسائط الإعلام الجماهيرية الحديثة وتركز صناعة الإعلام على فهم احتياجات العميل بميرون برينتون (Myron Brenton) إلى القول بأننا نعيش في "عصر أشبه بحوض السمك الزجاجي"، أصبحت فيه الحياة الخاصة ملكية عامة بفعل العبث بالبيانات الشخصية وتبادلها[2].

وثمة توتر بين الحق في حرية التعبير – ولا سيما ممارسة وسائط الإعلام لهذا الحق – والحق في الخصوصية. فحرية التعبير، سواء مارسها أفراد أو وسائط إعلام، والقدرة على ممارستها، هي سمة أساسية من سمات أي مجتمع يميزه الانفتاح وتعمه الحرية وينعم بالديمقراطية. حيث لا يمكن لأي مجتمع أن يطبق المسائلة الديمقراطية الحقيقة إلا من خلال ممارسة التعبير الحر، ولا يُقيد الحق في حرية التعبير ويمكن أن يصل إلى حماية حقوق الآخرين وحرياتهم. وهذا ميزان دقيق يكمن فيه الخط الرفيع بين التعبير الحر والخصوصية، وإن كان هو الميزان الذي تلجأ إليه المحاكم في التفاوض.

وفي الآونة الأخيرة، عُرفت الخصوصية بأنها حق الفرد في أن يقرر متى وكيف وإلى أي مدى يمكن تبادل المعلومات التي تخصه مع الآخرين[3] استجابة لقوة الكمبيوتر المتزايدة في المعالجة. ويقول ويستين (Westin) إن الخصوصية «هي حق الأفراد والجماعات والمؤسسات في أن يقرروا بأنفسهم متى وكيف وإلى أي مدى يمكن تبادل المعلومات الخاصة بهم مع الآخرين... [وهي] رغبة المرء في أن يختار بحرية في أي ظروف

---

1 بلوستين، (Bloustein) طبعة (1964) الخصوصية كجانب من جوانب الكرامة الإنسانية: إجابة على دين بروسر (Dean Prosser 39) المراجعة القانونية بجامعة نيويورك رقم 962

2 برينتون، إم (1964) (Brenton, M) المعتدون على الخصوصية

3 ويستين إيه إف (1967) (Westin AF) الخصوصية والحرية نيويورك: أثينيوم (Atheneum) صفحة 7

وإلى أي مدى يمكن الكشف عن بياناته وتوجهاته وسلوكياته إلى الآخرين".[4] ونوضح بمزيد من التفصيل في القسم 2 البعد الخاص الذي له أثر على الخصوصية التي نتج عنها الإنترنت: استعراض عالمي لتحديات وفرص حماية الخصوصية على الإنترنت.

لم تشغل قضية نوع الجنس اهتماماً يذكر في الجدل الدائر بشأن الخصوصية وتكنولوجيا المعلومات منذ تسعينيات القرن العشرين. فقد تمركزت المخاوف حول احتمالية التقنيات المعلوماتية التي تنتهك خصوصية النساء لأغراض جنسية و"الخصوصية القسرية" التي تفرضها الثقافات الأبوية على النساء والفتيات. وليس من هذه المخاوف ما هو أساسي فيما نناقشه بشأن الخصوصية من قضايا في هذه الورقة أو ممارسة حقوق الخصوصية الذي نتناوله في الأقسام اللاحقة. ولهذا تشير هذه الورقة للأفراد جميعاً وليس التفريق بين النساء والرجال وذلك من منطلق إيماننا بعمومية حقوق الخصوصية وانطباقها على الرجال والنساء على حد سواء.

ومع تغير مفاهيم الخصوصية تبعاً لتغير الظروف، لم تكن الأشكال الأولى من الحماية القانونية بمثابة أنظمة شاملة لصون الخصوصية، ولكن تمت الاستعانة بها في مواجهة مشاكل محددة في سياقات ومواقف معينة (قد نراها اليوم على أنها أوجه للحق العام في الخصوصية). ومن الأمثلة الأولى على مثل هذا النوع من تشريعات "الخصوصية" قانون «قضاة الصلح» المسمى England's Justices of the Peace Act لسنة 1361، والذي نص على اعتقال "مختلس النظر على عورات الغير" والمتنصت.[5] وجاءت القضية الرائدة إينتيك ضد كارينجتون (1765] (Entick v Carrington] والتي شكلت التعديل الرابع للدستور الأمريكي جاءت من منطلق الرغبة في حماية الأوراق المملوكة في أي منزل خاص. وركزت أمثلة أخرى على أغراض تصرف الحكومة في المعلومات الواقعة تحت حيازتها بشأن الأفراد (السويد) أو حظر نشر أنواع محددة من المعلومات الشخصية (فرنسا والنرويج).[6]

في القرن العشرين، عرفت المعايير القانونية الدولية الخصوصية على أنها حق من حقوق الإنسان. حيث ورد في الإعلان العالمي لحقوق الإنسان 1948 المحاولة الأولى لحماية الخصوصية كحق مميز من حقوق الإنسان، فنص في المادة 12 منه على ما يلي:

> «لا يُعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات".

لقد أثبت هذا الإعلان العالمي لحقوق الإنسان وبشكل كبير أنه إعلان ذو حجية، رغم عدم إلزامه قانونياً، ويمكن وجود الحق في الخصوصية في الكثير من وثائق حقوق الإنسان بما فيها الميثاق الدولي للحقوق المدنية والسياسية (ICCPR)، الملزم قانوناً والاتفاقية الأوروبية لحقوق الإنسان (ECHR). وسوف نتناول هذه الأمور بمزيد من التفصيل في القسم 3 عند استعراضنا للمعايير القانونية: البيئة القانونية والتنظيمية العالمية لحماية الخصوصية.

بالإضافة إلى هذه الأحكام الدولية الواسعة، أدخلت الكثير من الدول ضمن دساتيرها الحق في الخصوصية، وأخرى جعلته حكماً من أحكام بعض القوانين، وبعضها دفعت بمحاكمها للاعتراف بالحقوق في الخصوصية

---

4 المرجع السابق

5 بيريسفورد إيه و ستاجانو إف (2003) (Beresford A. and Stajano F.) خصوصية الموقع في الحوسبة المنتشرة، جمعية الاتصالات التابعة لمعهد مهندسي الكهرباء والإلكترونيات (IEEE)

6 منظمة المنظمة الدولية لحماية الخصوصية (،(2006 الخصوصية وحقوق الإنسان 2006: دراسة استقصائية دولية لقوانين وتطويرات الخصوصية

كحق دستوري ضمني، مثل الصين وألمانيا والهند.[7] وتتبع بعض أجهزة تعداد السكان بعض سياسات الخصوصية لضمان حماية المعلومات الشخصية التي يتم جمعها.[8]

وعلى الرغم من إجراءات الحماية المكثفة في الدساتير والقوانين على حد سواء، لا يزال الحق في الخصوصية من المفاهيم الغامضة شيئاً ما وسوف يعتمد ضمانه اعتماداً كبيراً على ظروف كل حالة بمفردها. ولقد ذكرت المحكمة الأوروبية: "إن المحكمة لا ترى من إمكانية أو ضرورة في محاولة وضع تعريف جامع لمفهوم "الحياة الخاصة»»[9]. حتى دفع انتفاء الوضوح أحد المعلقين إلى القول بأنه عندما "يبدو شيئاً ما خطأ ..... فإن هذا غالباً ما يكون الفاصل الأكثر فائدة بين معرفة متى يكون التدخل في الحياة الخاصة للفرد شيئاً معقولاً ومتى لا يكون كذلك"[10]. وحاولت مؤسسة الخصوصية الدولية (Privacy International) أن تضفي شيئاً من الوضوح على هذه المسألة من خلال تعريف الخصوصية بأنواعها المختلفة: خصوصية المعلومات (مثل البيانات الشخصية)، والخصوصية الجسدية (مثل الإجراءات العدائية)، وخصوصية الاتصال (مثل المراقبة)، وخصوصية المكان (مثل المسكن).[11] وفيما يتعلق بالإنترنت، تعتبر خصوصية المعلومات وخصوصية الاتصال هي الأكثر بروزاً.

ولكن يدل الاهتمام الذي يوليه الكثير من المشرعين والمفكرين للخصوصية على مر التاريخ إلى مدى أهميتها، ويعبر عن ذلك بولس شادويك (Paul Chadwick) (المفوض المعلوماتي لولاية فيكتوريا الاسترالية) إذا يقول: «الخصوصية هي أكثر حرياتنا هدوءاً ... الخصوصية كثيراً ما يطغى عليها في مناقشات السياسة العامة ... تلقى الخصوصية التقدير الأكبر عند غيابها، وليس عند وجودها".[12] ولقد تم التعبير عن قيمة الخصوصية على أساس قيمتها بالنسبة للفرد، فهي من أساسيات الكرامة الإنسانية والأفراد جميعاً، حتى قيل بأنه إذا كانت كل أفعالنا تراقب وتسجل فلن نستطيع أن نتصرف على طبيعتنا. ولقد تم التعبير عن الخصوصية كذلك على أساس فائدتها؛ حيث تعتمد الديمقراطية والحرية على تمتع الأفراد بقدر محدد من الخصوصية. ويعتبر الحق في الخصوصية هو أساس الكثير من حقوق الإنسان، الحق في حرية تكوين الجمعيات وحرية العقيدة وحرية التعبير التي تمثل أهم الأمثلة على ذلك. وكما يذكر أحد الكتاب: "جميع حقوق الإنسان بمعنى ما هي من أوجه الحق في الخصوصية"[13] من حيث أنه إذا لقيت الخصوصية الحماية اللازمة كانت كرامة الفرد مكفولة بناء على ذلك، وهذا هو أساس الحقوق والحريات الأخرى التي وضعت لحماية كرامة الشخص.

ولكن تجدر الإشارة إلى أنه حين ينشغل الناس دائماً بالخصوصية من حيث النظرية، فيبدو أنهم أقل اهتماماً بها من حيث التطبيق. حيث يتضح من الاستعمال العابر للإنترنت أن الأفراد يكشفون عن معلومات شخصية إلى درجة مذهلة للغاية. ولقد لاحظ الكثير تلك الفجوة بين ما يقول الناس بأنهم يأخذونه بعين الاعتبار وما يفعلونه على الإنترنت. فقد تكون هذه هي طبيعة الإنترنت التي يتم الدخول إليها في خصوصية وتجمع بين وسائط الاتصال في شكل بريد الكتروني (التي قد تعني إلى المستخدم خصوصية الهاتف أو المحادثة الخاصة) ووسائط الطباعة في بعض التطبيقات مثل الفيسبوك (Facebook). وثمة بعض الأدلة من الوقائع المختلفة على إدراك الأفراد لتداعيات الطباعة على الإنترنت ومدى إتاحة ذلك على المستوى العالمي وعدم القدرة

---

7 سولوف دي جي (Solove, D.J.) (2008) فهم الخصوصية، مطبعة جامعة هارفارد

8 مكتب الإحصاء الأمريكي، حماية البيانات وسياسة الخصوصية
http://www.census.gov/privacy/data_protection/our_privacy_principles.html

9 نيميتز ضد ألمانيا (Niemietz v Germany) (1992)، 16 EHRR 97. الفقرة 29

10 حسين جي (2006) "الخصوصية باعتبارها حرية" في آر جورجيرسين (محرر) "حقوق الإنسان في مجتمع المعلومات العالمي" مطبعة MIT، كامبريدج.

11 المنظمة الدولية لحماية الخصوصية، 2006.

12 المرجع السابق. الصفحة 2

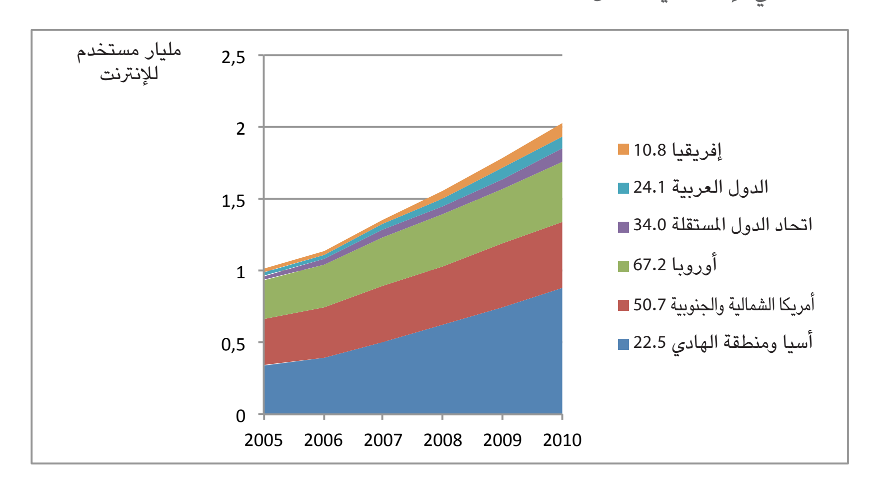
13 فوليو إف (Volio, F) "الشخصية القانونية والخصوصية والأسرة" في هينكين (Henkin) (محرر)، الشرعة الدولية لحقوق الإنسان (مطبعة جامعة كولومبيا 1981).

على مسحها. فعلى سبيل المثال، 57% من البالغين في الولايات المتحدة الذين يستخدمون الإنترنت يعتقدون خطأً بأنه عندما يطبق موقع من المواقع سياسة الخصوصية فإنه لن يشارك معلوماتهم الشخصية مع المواقع والشركات الأخرى.[14]

1.1. كيف غيرت الإنترنت من طبيعة التهديدات التي تتعرض لها الخصوصية؟ ما هي التهديدات الأساسية في العصر الرقمي؟

بدأ الوصول إلى الإنترنت في الاتساع بشكل سريع عبر معظم دول العالم. إذ تشير الإحصاءات الواردة من الاتحاد الدولي للاتصالات السلكية واللاسلكية (ITU)، الشكل 1، إلى أنه بين العام 2005 و 2010 فقط، تضاعف عدد المستخدمين للإنترنت. وفي العام 1995 فقط 0.4% من سكان العالم كانوا يستخدمون الإنترنت، وبحلول شهر مارس/ آذار 2011 ارتفعت هذه النسبة حتى وصلت إلى 30.2%.[15] وهو ما يعادل أكثر من ملياري مستخدم للإنترنت، 1.2 مليار منهم في الدول المتقدمة. كما كان استخدام الهواتف النقالة أكثر ارتفاعاً بكثير. ويظهر الشكل 2 عدد مستخدمي الهاتف النقال بين العام 1998 و 2009، فاليوم وصل عدد المستخدمين للهاتف النقال حول العالم 5.3 مليار مستخدم. كما أن الوصول إلى شبكات المحمول متوفر لـ 90% من سكان العالم، ويعتقد بعض المراقبين بأنه خلال الخمس سنوات القادمة قد تكون هذه الشبكات متاحة في كل أنحاء العالم.[16] وفي الدول المتقدمة، تزيد الاشتراكات في الهاتف المحمول عن عدد الأفراد (113.6 مشترك في كل 100 مواطن)، على حين أن العدد أقل بكثير في الدول النامية، إلا أنه في حد ذاته يعتبر مرتفعاً جداً: 56.8 مشترك في كل 100 مواطن.[17]

الشكل 1 [18] مستخدمي الإنترنت في مناطق مختلفة



---

14 تورو جي (Turow, J.) الأمريكيون والخصوصية على الإنترنت: تحطم النظام http://www.securitymanagement.com/archive/library/Anneberg_privacy1003.pdf

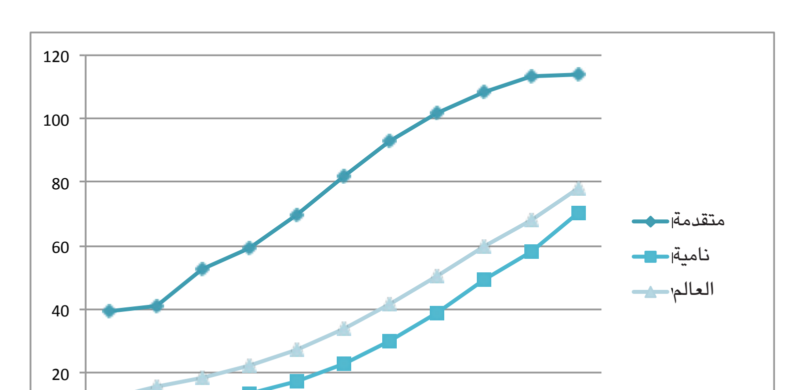
15 إحصاءات الإنترنت العالمية http://www.internetworldstats.com/emarketing.htm

16 انظر مثلًا سارازين تي (Sarrazin, T.) (2011) الرسائل النصية والتغريدات وإنترنت الهاتف المتنقل http://library.fes.de/pdf-files/bueros/africa-media/08343.pdf

17 ITU World Telecommunication 2010a. العالم في 2010. صفحة 4. [على الإنترنت] http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf

18 ITU World Telecommunication, 2010. ص.16.

الشكل 2 [19] عدد الاشتراكات في الهاتف المتنقل في كل 100 مواطن، 2000–2010



لقد نشأ عن الإنترنت والهاتف النقال معاً بيئة اتصالات رقمية عالمية سريعة التغير، وعلى الرغم من أن عدد صغير من الهواتف تدعم إمكانية استخدام الإنترنت وعدد أقل هو من الهواتف "الذكية"، إلا أن ذلك سيتغير بشكل سريع خلال الخمس إلى عشر سنوات القادمة؛ حيث يعتقد معظم المراقبين ارتفاع نسبة استخدام هذه الهواتف بشكل كبير. وفي حين كانت هناك تهديدات للخصوصية قبل العصر الرقمي بكثير، إلا أن التهديدات الحالية قد تغيرت بشكل كبير مع زيادة الإنترنت لقدرات الحكومات والشركات والأفراد على التدخل في خصوصية الآخرين. ويشير الكثير من المعلقين إلى أن نسبة كبيرة من الخصوصية التي كنا نتمتع بها في الماضي نشأت عن طبيعة الحياة – حيث كانت صعوبات مراقبة الأفراد معقدة ومكلفة جداً، ولم تتواكب التقنيات ولم تتوفر القدرة البشرية، وإن توفرت كانت مكلفة للغاية. ومع تطور الإنترنت وظهور الاتصالات الرقمية التفاعلية غير المكلفة، أصبحت القدرة على مراقبة الآخرين أسهل وأقل كلفة وأكثر فعالية. ولقد زادت الإنترنت وبشكل كبير من التأثير المحتمل على حقوق الخصوصية التي للشخص في هويته والتعامل مع بياناته الشخصية. ونتج عن استخدام الإنترنت والتعاملات التي تتم من خلالها قدر هائل من المعلومات الشخصية التي تعتبر حيوية لنموذج الأعمال في الشركات العاملة على الإنترنت – ويكمن التحدي الأكبر لصناع السياسة في كيفية فهمها أو تركها منظمة في بيئة عابرة للحدود تتسم بسرعة التغير.

إن الإنترنت بشكل عام:

- يمكن من جمع أنواع مختلفة من المعلومات الشخصية
- يسهل (وتطلب من الناحية الاقتصادية) جمع المعلومات الشخصية وتحديد موقعها
- يهيئ قدرات جديدة للحكومة والقطاع الخاص لتحليل المعلومات الشخصية
- يهيئ فرصاً جديدة للاستخدام التجاري للبيانات الشخصية
- ينتج عن تحديات جديدة بشأن التنظيم نظراً لطبيعتها العابرة للحدود القومية.

ونناقش فما يلي ما تتضمنه كل مسألة من هذه المسائل بالتفصيل.

---

19 ITU World Telecommunication, 2010. ص.16.

1.1.1. أنواع جديدة من المعلومات

لقد أدى التقدم التكنولوجي إلى استحداث أدوات تمكن من جمع وفهم أنواع من المعلومات كان يستحيل أو من غير الممكن الوصول إليها في الماضي. فمثلاً، لم يؤكد دور الحمض النووي (DNA) في الوراثة إلا في خمسينيات القرن الماضي، ولكن في الوقت الحالي سمح التقدم في العلوم الوراثية للعلماء استخلاص الحمض النووي من عينات أصغر بكثير، ومعرفة الكثير والكثير عن الفرد من خلال هذا الحمض النووي. ويمثل التخزين الرقمي للحمض النووي فائدة عظيمة في محاولات التصدي للجريمة، حيث مكن من ملاحقة عدد من القتلة المتهمين في جرائم قتل، وفي الوقت ذاته إطلاق سراح عدد من الأبرياء الذين تمت إدانتهم بغير حق. ولكن الاحتفاظ بالحمض النووي (DNA) له تأثيرات كبيرة على الخصوصية (من بين أمور أخرى) لأنه قد يحتوي على معلومات شخصية حساسة، مثل قابلية التعرض لأمراض معينة.

وثمة تطورات جديدة ذات أهمية في علم الاستدلال الحيوي (biometrics)، مثل التعرف على الوجه والمسح الضوئي للأصابع والمسح الضوئي للعين والتي انتشرت بشكل كبير كوسيلة للتعرف على الهوية. ولهذه الأجهزة الحيوية مجموعة واسعة من الاستخدامات – فهي تستخدم في منع التحايل من جانب تجار التجزئة وملاك المطاعم، وللتعرف على الناخبين في الانتخابات، ولتمكين المهاجرين من الدخول (بدلا من استخدام جوازات السفر)، واستيفاء سجلات الحضور في مكان العمل وللوصول إلى المناطق ذات الأمن المشدد. وعلى حين أن هناك قدر كبير من الفائدة الاجتماعية لهذه التطبيقات، فإن هناك أيضاً مخاوف تتعلق بمراقبة هذه البيانات الرقمية وبالأخص مسألة التخزين والوصول إليها. وكان هناك جدل خاص بشأن إجراء تصوير الجسم بالكامل في المطارات عقب محاولات الإرهاب لتهريب قنابل على متن طائرات داخل ملابسهم. واستنكر الكثير من المسافرين استخدام التقنيات التي تخترق الملابس وتظهر صورة عارية لهم يشاهدها الآخرون. واعتبرها البعض تعدياً على الخصوصية. حيث يمكن لهذه الصور أن تكشف عن معلومات شخصية جداً، مثل تعرض الفرد لعملية تجميل أو استخدامه لكيس فُغْرَة القولون، ولكن في الكثير من الأحيان يعتبر معظم الناس أن ملابسهم جزء أساسي من خصوصيتهم الجسدية. وهنا لابد من إيجاد توازن بين سلامة المسافرين وهذه المخاوف المتعلقة بالخصوصية، ولكن في هذه الظروف سريعة التغير يكون إيجاد التوازن الصحيح أمر غاية في الصعوبة.

جمع المعلومات الشخصية وتحديد موقعها

يختص كل جهاز كمبيوتر أو هاتف نقال أو أي جهاز آخر متصل بالإنترنت بعنوان بروتوكول إنترنت (IP) فريد يوفر محدد هوية فريد لكل جهاز، وهو ما يعني أنه يمكن تتبع هذه الأجهزة. فالقدرة على تحديد موقع أي جهاز من الأجهزة نشأ عنها تحديات كبيرة وجديدة بشأن الخصوصية. ومن أشهر الأدوات الكثيرة التي ابتكرت لتتبع مستخدمي الإنترنت ما يعرف باسم ملفات تعريف الارتباط (Cookies) وملفات التجسس (Web Bugs). حيث إن ملفات تعريف الارتباط (Cookies) هي عبارة عن أجزاء نصية صغيرة يخزنها متصفح الإنترنت على جهاز حاسوب المستخدم، وتقوم هذه الملفات "بالتسجيل" مع متصفح الإنترنت عند كل مرة يقوم فيها المستخدم بالدخول على هذا المتصفح ويمكن استخدامها في تتبع الجلسات وتخزين المواقع المفضلة وتصاريح الدخول وغير ذلك. ويمكن للمستخدمين أن يقبلوا أو يرفضوا هذه الملفات من خلال تغيير الإعدادات على برنامج المتصفح، ولكن هناك بعض المواقع لا يمكن استخدامها إلا بتفعيل ملفات تعريف الارتباط (Cookies). أما ملفات التجسس (web bugs) فهي ملفات لا يراها المستخدم عادة (حجمها 1×4 بكسل في العادة) وتكون مخفية ضمن صفحات الإنترنت والرسائل الإلكترونية. وعند الاطلاع على الصفحة/ الرسالة الالكترونية المحتوية على ملف التجسس (web bug)، يقوم هذا الملف بإرسال معلومات إلى الخادم (تشتمل على عنوان بروتوكول الإنترنت (IP) الخاص بالمستخدم، وموعد وتاريخ الدخول على الصفحة/ فتح الرسالة الالكترونية ونوع المتصفح المستخدم).

يمكن ربط عنوان بروتوكول الإنترنت (IP) بهوية الشخص الفعلية بكثير من الطرق. فقد طورت الكثير من مواقع الإنترنت ومزودي خدمات الإنترنت أنظمة التحقق من المستخدم تتضمن الكشف عن الهوية (خاصة خلال التعاملات التجارية الالكترونية)؛ وتتطلب الكثير من التطبيقات عنوان البريد الالكتروني الشخصي أو أشكال أخرى من تحديد الهوية، وقد تطلب الحكومة من مستخدمي الإنترنت تسجيل عنوان بروتوكول الإنترنت (IP) الخاص بهم، ويمكن أحياناً الحصول على الهوية من خلال تحركات الشخص على الإنترنت (انظر أدناه).

من السمات الأساسية في الإنترنت إمكانية التفاعل مقارنة بالتقنيات "القديمة" مثل التلفاز والراديو والهاتف. ويطلب من المستخدمين دائماً تقديم معلومات عن أنفسهم في كل خطوة – مثلاً، ما هو البحث المراد، ما هي الروابط التي ينقرون عليها، وما هي الصفحات التي اطلع عليها ومدة فتحه لهذه الصفحات. وهناك سلسلة من الأدوات والأجهزة التقنية التي صممت لجمع هذه المعلومات (مثل: TiVo وXbox360 وGoogle Books)[20]. وهذه التقنيات هي من أساسيات النموذج الاقتصادي للإنترنت. كما إن رقمنة المعلومات (Digitalisation of Information) وتوقع حرية الدخول يجعل من الأشكال التقليدية لتحقيق الدخل أمراً أكثر تعقيداً على الإنترنت، ومن ثم تقوم الشركات الناجحة "بالتنقيب" عن البيانات الشخصية حتى تستهدف المستخدمين بدعاياتها. ولهذا يوجد حافز اقتصادي مباشرة وقوي لتأمين البيانات الشخصية والاحتفاظ بها ومشاركتها. وينطبق هذا أيضاً على النشاط الالكتروني غير المتصل بالإنترنت، حيث يمكن استخدام الشفرة العمودية الحاسوبية (Bar Code) في تتبع مشتريات الأفراد وتستخدم بعد ذلك في التحكم في مستويات المخزون وحوافز الاستهداف أو التسويق لهؤلاء العملاء. وتوفر بطاقات السفر الحاسوبية مثل بطاقة London Oyster صورة رقمية عن كل رحلة ويمكن استخدامها في رصد تحركات المسافر في كل مناطق المدينة – وتكون مفيدة لتخطيط التنقل وكذلك لتتبع رحلات الأفراد. ومع تزايد استخدام الإنترنت في التعاملات اليومية مثل الأعمال المصرفية والتسوق والحياة الاجتماعية مع الآخرين، يزداد كذلك الإفصاح عن البيانات الشخصية، غالباً دون قصد، بما فيها معلومات حساسة عن الماليات والصحة وحتى عن الميول الجنسي. وتسمح هذه التطورات إلى زيادة حجم المعلومات المجمعة، وكما يوضح لورينس ليسيج (Lawrence Lessig)، " تصبح حياة المرء سجلاً متزايداً باستمرار"[21].

كما أصبحت مشاهدة الأشخاص وتحديد مواقعهم دون اتصال أمراً سهلاً باستخدام المراقبة الالكترونية، حيث تستخدم كاميرات المراقبة والأقمار الصناعية في رصد الأماكن العامة والخاصة، وهي متوفرة للكثير والكثير من الأفراد. ومن ثم أصبحت المعلومات المتعلقة بالأماكن رخيصة إلى حد بعيد من خلال المبادرات الخاصة مثل GoogleEarth. وأصبحت أنظمة تحديد المواقع العالمية (GPS) مدمجة في الكثير والكثير من أجهزة العملاء. وتعد رقاقات التعرف على الهوية بالترددات اللاسلكية (RFID) مثالاً آخر على هذه الأجهزة، والتي كانت باهظة الثمن في البداية، ولكن بدأت أسعارها في الانخفاض وفي النهاية أصبحت لا تكشف فقط عن المنتج الذي يشتريه المستهلك ولكن أيضاً عدد مرات استخدامه ومكان الاستخدام.[22]

3.1.1. قدرات جديدة للمعنيين في القطاع الخاص لتحليل البيانات

تعني القوة الحاسوبية الزائدة أنه يمكن بدون تكلفة وبشكل فعال تخزين كميات هائلة من المعلومات ودمجها وتحليلها بمجرد جمعها. ويسمح التقدم التكنولوجي بالربط بين قواعد بيانات المعلومات مع بعضها البعض، الأمر الذي يتيح إمكانية معالجة قدر أكبر من البيانات. وتزداد احتمالية انتهاك الخصوصية

---

20 المنظمة الدولية لحماية الخصوصية .2006 ،(Privacy International)

21 ليسيج لورينس (1999) (.Lessig, L) "مدونة وقوانين الفضاء الالكتروني" Basic Books، نيويورك. صفحة 152.

22 مارتينيز-كابريرا، إيه (2010) (.Martínez-Cabrera, A) تزايد مخاوف الخصوصية مع استخدام رقاقات RFID http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/09/05/BUCE1F8C1G.DTL

بشكل كبير عند جمع التكنولوجيا معاً، فربطت قواعد بيانات التعرف على الوجه (كما هو مستخدم على الفيسبوك (Facebook)) مع كاميرات المراقبة مثلا يسمح بتتبع الأفراد بمستوى غير مسبوق.

لقد انتشرت عملية دمج وتكامل قواعد البيانات المعلوماتية المختلفة. وتنشأ مسائل الخصوصية كما هو واضح عند تطابق البيانات من مصادر مختلفة، مثلاً تطابق بيانات الضريبة مع بيانات الصحة أو بيانات المالية مع بيانات الضمان الاجتماعي. ويمكن استخلاص البيانات الشخصية من التقنيات المختلفة ثم مطابقتها بالبيانات المتوفرة للعامة لتكوين ملف شخصي مفصل.

يذكر مركز معلومات الخصوصية الالكترونية (EPIC) الذي يتخذ من الولايات المتحدة مقراً له: "يعزم القائمون بجمع معلومات المستهلكين على تصنيف أية معلومة وجمعها وبيعها الكترونياً". على سبيل المثال، تقوم شركة Medical Marketing Service ببيع قوائم الأفراد الذين يعانون من عدت أمراض، وتكون هذه القوائم مرتبطة بإشارة مرجعية مع المعلومات المتعلقة بالعمر والمستوى التعليمي وحجم الأسرة ونوع الجنس والدخل وأسلوب الحياة والوضع الاجتماعي ووجود أطفال. وتشتمل قائمة الأمراض على ما يلي: مرض السكري وسرطان الثدي وأمراض القلب. وتبيع الشركات الأخرى قواعد بيانات تحتوي على معلومات تتعلق بعادات حياة الأفراد وما يفضلونه من كتب وحتى معتقداتهم الدينية".[23]

ولقواعد البيانات المجمعة العديد من الاستخدامات. حيث يمكن استخدامها في التنقيب عن البيانات، التي هي عبارة عن "عملية البحث عن أنماط المعلومات التي تحتويها قواعد البيانات".[24] ولتنقيب البيانات الكثير من الاستخدامات، حيث تفيد في تحديد الأنماط التي تدل على استخدام بطاقة الائتمان من أجل الاحتيال. وعلى حين يدعي بعض المراقبين بأن التنقيب عن البيانات هو عملية حيادية، إلا أنه قد ينتج عنها بعض التداعيات على الخصوصية. فغالبا ما يتضمن التنقيب عن البيانات ودمجها استخدام معلومات عن الأفراد بطريقة غير راضين عنها وغير مدركين لها. فضلاً عن أن المجموعة الواسعة من البيانات التي يعتمدون عليها تتضمن تفاصيل شخصية ويمكن ربطها بسهولة بأفراد دون معرفتهم.

من الاستخدامات الأخرى العامة تصنيف البيانات في ملفات تعريفية، وهي استخدام البيانات المصنفة في "تحديد وفصل وتصنيف واتخاذ القرارات بشأن أفراد معروفين إلى متخذ القرار فقط من خلال الملف المعد لهم على الحاسب الآلي".[25] ويمكن للشركات والحكومات استخدام هذه العملية لبناء ملفات شاملة عن الأفراد. ويعطي مركز معلومات الخصوصية الالكترونية (EPIC) مثالاً عن سيدة رفعت قضية ضد شركة متروميل (Metromail) التي تتخذ من الولايات المتحدة مقراً لها بعد أن لاحقها أحد موظفي إدخال البيانات على أساس المعلومات التي تقدمت بها في الدراسة الاستقصائية. وخلال القضية، تبين أن الشركة قد احتفظت بملف مكون من 25 صفحة يتعلق بالسيدة ويشتمل على "دخلها ومعلومات عن موعد استخدامها لعلاج البواسير".[26]

---

23 روتينبيرج إم و هوفناجل سي (Rotenburg M. And Hoofnagle C.) الخضوع إلى لجنة الإصلاح الحكومية التابعة لمجلس النواب بشأن التنقيب عن البيانات" 25 مارس/ آذار2003 / http://epic.org/privacy/profiling/datamining3.25.03.html

24 فاياد يو، جرينستين، جي، و ويرس إيه (Fayyad, U., Grinstein, G. and Wierse, A.) (2001) "إظهار المعلومات في التنقيب عن البيانات واكتشاف المعرفة". Morgan Kaufman Publishers.

25 نيتر دابليو (Netter, W) "موت الخصوصية" نمط الخصوصية 1: تقديم لتشكيل البيانات، جامعة هارفارد، 2002 http://cyber.law.harvard.edu/privacy/Module2_Intro.html

26 مركز معلومات الخصوصية الالكترونية (EPIC)، "الخصوصية وتصنيف بيانات المستهلكين في ملفات تعريف"/ http://epic.org/privacy/profiling/

ولحماية الخصوصية (والتحايل في نفس الوقت على قوانين الخصوصية)، تقوم الشركات غالباً بإلغاء تعريف الأفراد أو بطمس تفاصيل هويتهم من البيانات. وهي عملية تصفية البيانات من التفاصيل الشخصية (مثل الاسم ورقم التأمين الاجتماعي ورقم بروتوكول الإنترنت (IP)). ولكن، تُظهر الدراسات بأنه دائماً ما يكون من الممكن ربط المعلومات "غير المحددة الهوية" بصاحبها مرة ثانية. فمثلاً، كشفت دراسة أجريت في عام 1990 في الولايات المتحدة الأمريكية أن البيانات التي تم جمعها خلال التعداد السكاني (مثل الرمز البريدي وتاريخ الميلاد ونوع الجنس) يمكن ربطها بإشارة مرجعية ويمكنها أن تحدد وبشكل فريد 87% من السكان القوميين.[27] وظهر مثال آخر في العام 2006 عندما أطلقت شركة إيه أو إل (AOL) بيانات بحث عن المستخدم كانت غير قابلة لتحديد الهوية، فتمكن الباحثون عندئذ من تحديد الكثير من المستخدمين من خلال الظاهرات المعتادة للبحث عن أنفسهم، حيث كان يبحث الفرد عن بياناته الشخصية.[28]

قد يكون من الصعب جداً حماية قواعد البيانات، ولا سيما عندما يسهل الوصول إليها عن بعد وعند حرية الكثير من الناس في الوصول إليها. مما يجعل البيانات الشخصية في قواعد البيانات معرضة لجرائم الإنترنت بكل ألوانها. ويضاف إلى ذلك أن المعلومات عادة ما تخرج إلى نطاق الملكية العامة. ولهذا أسباب مشروعة، وإن نتج عنه مشاكل تتعلق بالخصوصية. مثلاً، قاعدة بيانات WHOIS تحتوي على تفاصيل الاتصال الشخصية للفرد أو المؤسسة التي سجلت كل اسم نطاق. ويتم نشرها للعامة كي تسمح لمديري الشبكات بإصلاح المشكلات على الإنترنت بكل سهولة.[29] وهناك مثال آخر وهو الانتقال في الكثير من الدول لنشر سجلات عامة في صيغة رقمية. وتحتوي هذه السجلات على معلومات كانت متاحة قبل ذلك (مثل شهادة الميلاد والزواج والوفاة) ولكن الصيغة الجديدة التي نشرت بها جعلت من السهل أكثر الحصول عليها والرجوع إليها.[30]

4.1.1. قدرات جديدة للحكومات لتحليل المعلومات الشخصية

بدأت الحكومات في السعي إلى تسخير قوة الإنترنت في تنفيذ مهامها. فشهدت السنوات الأخيرة تحولاً دراميا تجاه الحكومة الالكترونية كوسيلة من وسائل تقديم الخدمات الأكثر توفيراً للتكلفة والملبية للمتطلبات الخاصة. ونتيجة لذلك، بدأت الكثير من الدول في سعيها نحو تسهيل وتنسيق تقديم الخدمات من خلال تطوير قواعد بيانات ضخمة تحتوي على معلومات شخصية عن المواطنين. حيث تستخدم بطاقات الهوية، على سبيل المثال، بشكل أو بآخر في كل دول العالم بشكل افتراضي، وتستخدم بطاقات الهوية القومية الإلزامية في ما يقرب من 100 دولة.[31] وبدأت الحكومات وبوتيرة سريعة في الاتجاه نحو جمع المعلومات الحيوية على البطاقات وتخزينها في قواعد بيانات ضخمة يمكن استخدامها في السماح بالدخول إلى التأمين الاجتماعي أو الصحة أو في السفر ومراقبة تحركات المستخدم على سبيل المثال.

---

27 سويني إل (Sweeney, L) "إستراتيجيات طمس هوية الشخص من بيانات المرضى لأغراض البحث" جامعة كارنيجي ميلون، معمل خصوصية البيانات، 1998 http://www.ocri.ca/ehip/2005/presentations/Sweeney_bw.pdf صفحة 26.

28 سوغويان سي (2007) (Soghoian, C.) "إشكالية البحث عن البيانات الذاتية المجهولة" جامعة إنديانا بلومنجتون – جامعة المعلوماتية. نشر على الإنترنت http://papers.ssrn.com/sol3/papers.cfm?abstract_id=953673 صفحة 1.

29 مركز معلومات الخصوصية الالكترونية "WHOIS" الوصول إليه 15/03/10، نشر على الإنترنت http://epic.org/privacy/whois/

30 المنظمة الدولية لحماية الخصوصية (Privacy International)، 2006).

31 المنظمة الدولية لحماية الخصوصية (Privacy International)، 1996)، الأسئلة الأكثر تكراراً بشأن بطاقات الهوية https://www.privacyinternational.org/article/id-card-frequently-asked-questions

وثمة دور مهم جداً لهذه التقنيات في مجال منع الجريمة وملاحقة المجرمين. وحتى قبل "الحرب على الإرهاب" كانت الكثير من الحكومات تستفيد أقصى استفادة من تقنيات المراقبة مثل كاميرات المراقبة لتحقيق هذه الأهداف. ومنذ أحداث الحادي عشر من سبتمبر/ أيلول، تحول تهديد الإرهاب إلى دافع في الكثير من البلدان لزيادة استخدام أساليب المراقبة غالباً بوسائل تدخليه، بل ومنتهكة لقوانين الخصوصية القائمة. ومن الأمثلة الوثيقة الصلة على ذلك السفر جواً، فكما أشرنا سابقاً، تستخدم أجهزة مسح الجسم بالكامل أو يتم تجربتها في الولايات المتحدة الأمريكية والمملكة المتحدة وأيرلندا الشمالية والهند واستراليا واليابان وروسيا الاتحادية وهولندا من بين دول أخرى.[32] ومن الممارسات الأخرى استخدام قوائم المراقبة السرية، مثلما كان في كندا والولايات المتحدة الأمريكية.[33] حيث يقوم المسافرون بتقديم البيانات الشخصية كشرط من شروط السفر ثم يتم التحقق من هذه المعلومات بمقارنتها بقواعد البيانات من مصدر معين. وتستخدم وظيفة تشكل البيانات في إنشاء قوائم للأفراد المصنفين على أنهم تهديد للأمن، ويتم تعميم القائمة على الدول الأخرى ثم يتم منع الأفراد من السفر أو إخضاعهم إلى تدابير أمنية معززة. وأحياناً تم نشر قوائم المراقبة بشكل عام؛ مما أظهر بعض الأخطاء، ولكن شوه سمعة بعض الأفراد؛ وأحياناً يتم حفظها سراً ما يعني حرمان بعض الأفراد من التأشيرة دون إدانتهم بالضرورة بأي شيء أو منحهم الفرصة للدفاع عن أنفسهم.[34] وفي إحدى القضايا الشهيرة في المملكة المتحدة وأيرلندا الشمالية، مُنع مواطن مسلم بارز يُدعى يوسف إسلام (وهو المغني السابق الذي كان يدعى كات ستيفينز) من السفر إلى الولايات المتحدة الأمريكية (حيث إن الرحلة التي كانت على متن طائرة شركة يونايتد إيرلاينز (United Airlines) التي كانت متجهة من لندن إلى مطار دوليس إنترناشونال إيربورت (Dulles International Airport) بواشنطن تم تحويل اتجاهها إلى بانجور، ماين، عندما اكتشف مسؤولون أمريكيون بعد الاطلاع على قائمة الركاب أنه على متن الطائرة)، وذلك لوجود ادعاءات بأن له صلة بروابط إرهابية، ولكن لم تكن صريحة على الإطلاق، رغم سجله كمسلم يدعو إلى السلام والتسامح بين الناس. وبعد ذلك رُفع عنه الحظر.

استطاعت بعض الحكومات أن تستخدم هذه التقنيات في مراقبة أعمال المواطنين، ولا سيما المعارضين بشكل أكثر كثافة. فعلى سبيل المثال، ذكرت مبادرة OpenNet Initiative أنه يتم في الصين تشغيل جهاز الرسال الفورية الأكثر شيوعاً على الإنترنت (QQ) لتسجل اتصالات المستخدم على الإنترنت وإبلاغها إلى الشرطة. وفي العام 2006، أعلنت وزارة الأمن العام الصينية عن إطلاق مشروع "الدرع الذهبي" (Golden Shield) الذي صمم ليكون بمثابة نظام قومي للمراقبة الرقمية. وفي العام 2008 كشف شركة هاتف نقال حكومية عن قدرتها غير المحدودة في الوصول إلى معلومات عملائها وتقديمها إلى الحكومة الصينية عند الطلب. وكان أكثر الأمثلة بروزاً محاولة الحكومة الصينية في العام 2009 إصرارها على تثبيت نظام يعرف باسم السد الأخضر (Green Dam) في أجهزة الكمبيوتر الشخصية المباعة في الصين.[35] وكان في استطاعة هذا النظام مراقبة تحركات أجهزة الكمبيوتر الشخصية من خلال تركيب بعض المكونات في نظام التشغيل وإعطاء السلطات الصلاحية المباشرة في مراقبة المحتوى والاطلاع عليه (والسماح كذلك بالتحكم في الحاسب الآلي عن بعد).[36] ولكن لم تتم الموافقة على المقترح في نهاية المطاق من خلال منظمة التجارة العالمية (WTO) لأسباب تجارية.

32 كافوكيان إيه (Cavoukian, A) "تصوير الجسد بالكامل في أجهزة المسح الضوئي بالمطارات": بناء الخصوصية من خلال التصميم" مفوض المعلومات والخصوصية، أونتاريو، كندا. يونيو 2009 http://www.ipc.on.ca/images/Resources/wholebodyimaging.pdf صفحة 2.

33 مجلس حقوق الإنسان، الجلسة الثالثة عشر، بند جدول الأعمال رقم 3. 28 ديسمبر/ كانون الأول 2009، A/HRC/13/37 http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf صفحة 17.

34 المرجع السابق.

35 مبادرة Opennet Initiative، السد الأخضر الصيني: تداعيات تعدي الحكومة على الكمبيوتر الشخصي المنزلي http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc

36 وولشوك، إس؛ ياو آر، وهالدرمان إيه (2009) (Wolchok, S.; Yao, R. and Halderman, A.) تحليل نظام برمجيات رقابة السد الأخضر. http://www.cse.umich.edu/~jhalderm/pub/gd/

ومؤخراً، أفادت أنباء عن محاولة بعض السلطات الصينية إنشاء مقاهي وفنادق وأعمال أخرى في وسط بكين بغرض تركيب تقنية مراقبة للمستخدمين لخدمة الإنترنت اللاسلكي (Wi-Fi) التي اعتبرت مثالا آخراً على تقييد حرية استخدام الإنترنت.[37]

أشار المقرر الخاص المعني بمكافحة الإرهاب وحقوق الإنسان إلى أمثلة عن ممارسات المراقبة في ألمانيا وكولومبيا وبنجلاديش والولايات المتحدة الأمريكية والتي أثارت قلقه.[38] وكشفت دراسة أجرتها مؤسسة الخصوصية الدولية Privacy International في العام 2007 عن تدهور الوضع العام لحماية الخصوصية وصونها، فضلاً عن زيادة المراقبة في 47 دولة.

وتعد جرائم الفضاء الالكتروني من المشكلات المتزايدة على الإنترنت، حيث تشير التقديرات إلى أن تكلفة السرقة على الإنترنت بلغت 1 تريليون دولار.[39] ويمكن لتدابير الأمن المتراخية وخروق الأمن أن تنتج عن قيام المجرمين بسرقة بيانات الأفراد التي يستخدمونها في ارتكاب الكثير من الجرائم مثل التحايل والسرقة والملاحقة.

وأخيراً، تستخدم تقنيات المراقبة بشكل أكبر على المستوى المحلي في رصد سلوك أفراد الأسرة والموظفين. وبدلاً من مراقبة الموظفين الذين يظهرون سلوكاً مريباً، بدا من الواضح قيام أصحاب العمل بإنشاء مراقبة دائمة لمكان العمل.[40] كما أن السوق لا يكف عن تطوير تقنيات جديدة تساعد أصحاب العمل في مراقبة الموظفين، والمثال على ذلك تطوير تقنية جديدة مؤخراً تمكن من الكشف عن سلوك الموظف المعقد وتبلغ صاحب العمل به - حيث يمكن للجهاز التمييز بين الحركات المختلفة مثل "الفرك والمسح والمشي وحتى إفراغ سلة المهملات".[41]

5.1.1. فرص جديدة للاستخدام التجاري للبيانات الشخصية

لقد نتج عن الإنترنت كم هائل من الأنشطة الاقتصادية، وتقدر دراسة أجراها مؤخراً معهد McKinsey أن التأثيرات الاقتصادية المباشرة وغير المباشرة للإنترنت تمثل 3.4% من إجمالي الدخل القومي في 13 دولة خضعت للدراسة ولكن 21% من النمو الاقتصادي في خمسة اقتصادات ناضجة، مع توفير 2.6 فرصة عمل لكل وظيفة يتم فقدها.[42]

تتمتع شركات الإنترنت مثل جوجل (Google) وياهو (Yahoo) والفيسبوك (Facebook) بحرية الوصول إلى كم هائل من البيانات.[43] وهي أكثر شركات الإنترنت التي لديها قواعد مستخدمين هائلة

---

37 براناجان تي (2011) (Branagan, T.) الصين تعزز من مراقبة الإنترنت http://www.guardian.co.uk/world/2011/jul/26/china-boosts-Internet-surveillance

38 مجلس حقوق الإنسان، 2009/19/20

39 ويبير تي (Weber, T.)، ازدياد تهديد جريمة الفضاء الالكتروني بشكل حاد، بي بي سي نيوز، 31/01/09 http://news.bbc.co.uk/1/hi/business/davos/7862549.stm

40 بونسور كي (Bonsor, K.) هل تخضع أنشطتك على الكمبيوتر إلى المراقبة في مكان عملك؟ http://computer.howstuffworks.com/workplace-surveillance1.htm

41 فيتزباتريك إم (Fitzpatrick, M) "الهاتف المتنقل الذي يسمح للمديرين التلصص على الموظفين"، بي بي سي نيوز، 2010/03/10 http://news.bbc.co.uk/1/hi/technology/8559683.stm

42 معهد McKinsey Global Institute، (2011)) مسائل الإنترنت: أثر الإنترنت الكاسح على النمو والوظائف والازدهار http://www.eg8forum.com/fr/documents/actualites/McKinsey_and_Company-internet_matters.pdf

43 ماسيمينو إيه (Massimino, E.) (2012) الخصوصية، التعبير الحر ومعيار الفيسبوك http://www.forbes.com/sites/realspin/2012/01/31/privacy-free-expression-and-the-facebook-standard/

(مثلا الفيسبوك (Facebook) لديها ما يزيد على 800 مليون مستخدم[44]) وتمتد لتشمل المزيد والمزيد من التعاملات، (مثلاً: يمكن للمستخدم استخدام جوجل (Google) في التوصل إلى الإنترنت، وإرسال الرسائل الالكترونية وعرض مقاطع الفيديو والتسوق وخلافه). والكثير من الخدمات التي تقدمها هذه الشركات هي مجانية وتعتمد نماذج عملها على جمع معلومات المستخدم واستخدماها لأغراض التسويق. ولذلك تمثل بيانات المستخدم قيمة اقتصادية كبيرة. وقد كشفت دراسة أجريت في عام 1999 أن 92% من مواقع الإنترنت كانت تجمع على الأقل نوع واحد من المعلومات المحددة للهوية عن مستخدميها (مثل الاسم أو عنوان البريد الالكتروني أو العنوان البريدي)[45]، ويمكن التأكيد على أنه منذ ذلك الحين ازدادت عملية جمع المعلومات. وتوجهت الشركات كذلك إلى أن تمارس أقصى درجات السرية بشأن نوع المعلومات التي تجمعها وكيفية جمعها، كما ذكرت مجلة ذي إكونوميست (The Economist)، وذلك لأن الأمر يتعلق بالميزة التنافسية بذات قدر تعلقه بمخاوف الخصوصية.[46]

تعتمد جل هذه الأنشطة الاقتصادية على وسطاء الإنترنت – مجموعة من أصحاب المصلحة والخدمات والتطبيقات التي تسهل من التعاملات بين الأطراف الأخرى على الإنترنت، بما في ذلك على سبيل المثال محركات البحث ومزودي خدمات الإنترنت. وتعتمد الاتصالات من خلال الإنترنت اعتماداً متزايداً على هؤلاء الوسطاء للوصول إلى البيانات ومعالجتها وإرسالها. ولقد نشأ عن القوة المتزايدة للوسطاء وتحكمهم في البيانات الشخصية عدداً من المخاوف بشأن ما إذا كانت التنظيمات السارية كافية لحماية حقوق الخصوصية. وكان من بين هذه المخاوف ثلاثة أنواع بارزة – مواقع التواصل الاجتماعي، والحوسبة السحابية ومحركات البحث.

مواقع التواصل الاجتماعي

مواقع التواصل الاجتماعي هي عبارة عن مواقع الكترونية تركز على بناء و/أو إظهار العلاقات الاجتماعية بين الأفراد. تعمل بعض هذه المواقع على تسهيل "الصداقات" الافتراضية مع الأفراد المعروفين بالفعل للمستخدم في الواقع، مما يسمح لهم بمشاركة الصور وتبادل الحديث على الإنترنت. ويركز البعض الآخر على السماح للأفراد أن يكونوا صداقات، غالباً مع تركيز خاص على مجال معين مثل علاقات العمل (LinkedIn) أو أذواق الموسيقى (Pandora). وتختلف كل خدمة من الخدمات عن الأخرى، ولكن يسمح النموذج الموحد للمستخدمين بإنشاء صفحتهم الخاصة بهم والتي تحتوي على بعض المعلومات الشخصية (مثل تاريخ الميلاد ومكان التواجد والاهتمامات والاسم) ويمكن بعد ذلك للمستخدمين الارتباط مع أصدقاء سيتمكنون عندئذ من رؤية معلومات بعضهم البعض. وتنتشر مواقع التواصل الاجتماعي بشكل كبير مع استقطاب مئات الآلاف من المستخدمين بينهم. ولكن كان هناك قلق متزايد بشأن انتهاكات الخصوصية التي تسببت فيها هذه المواقع، وتتعلق بعض هذه المخاوف بمعرفة كيفية استخدام وسائط الإعلام والاتصالات، حيث إن الكثير من المستخدمين غير مدركين لمخاطر الكشف عن المعلومات الشخصية إلى الآخرين. ولا يمارس الكثير من المستخدمين أي قيود في السماح لأي شخص برؤية بياناتهم، ويكون الكثير من المستخدمين صداقات مع أفراد لا يعرفونهم بشكل كاف. قد يكون لهذا تداعيات كبيرة عندما يكون مثلاً للمستخدم 130 صديق على موقع الفيسبوك (Facebook). [47] ونناقش هذا الأمر بمزيد من التفصيل في القسم التالي.

---

[44] بروتالانسكي إيه (Protalanski, E.) (2012) يبلغ عدد مستخدمي الفيسبوك 845 مليون مستخدم. https://www.zdnet.com/blog/facebook/facebook-has-over-845-million-users/8332

[45] لجنة التجارة الفيدرالية، (1999) "التنظيم الذاتي والخصوصية على الإنترنت: تقرير إلى الكونجرس" مارس/آذار1999, نشر على الإنترنت http://www.ftc.gov/os/1999/07/privacy99.pdf صفحة 4.

[46] (Economist، 2010) " النقر بحثاً عن الذهب: كيف تحقق شركات الإنترنت فوائد من البيانات على شبكة الإنترنت"، في "تقرير خاص حول إدارة المعلومات"، مجلة The Economist، المجلد 394، رقم 8671

[47] الفيسبوك (2012) ،(restraint) "إحصاءات" نشرت على الإنترنت http://www.facebook.com/press/info.php?statistics

الحوسبة السحابية

الحوسبة السحابية هي عبارة عن هيكل شبكات ناشئ يتم من خلاله تخزين البيانات أو طاقة المعالجة أو البرامج في أجهزة خادم عن بعد، على خلاف أجهزة الكمبيوتر الشخصية، وتكون متاحة من خلال الإنترنت. وتتوفر أشكال مختلفة من الحوسبة السحابية وتوفر مجموعة كبيرة من الخدمات. ويمكن للأفراد أو المنظمات تأجير القدرة الحاسوبية بشكل فعال من مزودي الخدمة عن بعد. فمثلاً، تسمح خدمة تطبيقات جوجل (Google's Apps) للأفراد بإنشاء وحفظ مستندات معالجة spreadsheet وword على الإنترنت. وتشتمل بعض الخدمات الأخرى على منصات تعاونية تسمح للمستخدمين حرية الوصول إلى المستندات بشكل فوري، مثل منصات wiki ومستندات Google docs. [48]

ويمكن أن يكون للحوسبة السحابية عدة فوائد إيجابية: مثلاً، يمكن أن تقلل من تكاليف شراء وتحديث البرامج للشركات والمؤسسات الصغيرة، حيث أنها تدعم تحديداً المستخدمين الذين يحظون بمستويات متدنية من الموارد المالية في الدول النامية. كما إنه يمكنها تحسين سبل الراحة للمستخدمين من خلال السماح لهم بالوصول إلى المستندات في أي مكان في العالم، وتأليف المستندات بالتعاون مع الآخرين في مواقع جغرافية مختلفة.

ولكن، تثير الحوسبة السحابية كذلك عدداً من المخاوف من منظور الخصوصية. حيث يتم تخزين البيانات في جهاز طرف ثالث يتحمل المسؤولية عن حمايتها ويفقد المستخدم قدرته على التحكم فيها. يضاف إلى ذلك أن القوانين التي تغطي الحوسبة السحابية غير محددة بما يكفي لذلك فليس هناك ما يضمن خصوصية بيانات المستخدمين. أحياناً تذكر شروط وأحكام الاستخدام أن لمزود الخدمة القدرة على إنهاء الحسابات وإزالة/ تحرير المحتوى وفق إرادته. مثلاً، هذه هي الحالة في موقع Mozy.com، تلك الخدمة التي تسمح للمستخدمين جمع المعلومات وتخزينها على أجهزة الكمبيوتر الخاصة بهم على الإنترنت.[49] هذا يعرض المستخدمين لخطر فقدان معلوماتهم الشخصية. وتقيد الكثير من الشروط والأحكام من قدرة مزود الخدمة، وهو ما يعني أنه في حال وجود خرق في الأمن وفقدان المستخدمين لبياناتهم الشخصية فلن يحصلوا على أي تعويض. وأخيراً لا يهتم مزودو الخدمة في الغالب بما يحدث لمعلومات المستخدم بمجرد إغلاقهم للحساب أو مسحه. وهذا لا يعني دائماً إزالة المعلومات، مما قد يؤدي إلى خرق الخصوصية.[50] سنناقش تداعيات الحوسبة السحابية على الخصوصية بمزيد من التفصيل في القسم التالي.

محركات البحث

تقوم محركات البحث بتنفيذ دور حيوي كوسيط على الإنترنت يسمح للأفراد البحث عن المحتويات والاطلاع عليها، ومن أمثلة هذه المحركات Google وBing وAsk.com وYahoo! Search. وتقوم محركات البحث في العادة بجمع قدر هائل من البيانات الشخصية بما في ذلك عناوين بروتوكول الإنترنت (IP) وطلبات البحث والوقت والتاريخ والمكان الذي قدم فيه جهاز الكمبيوتر الطلب. وكما سبق وناقشنا، يمكن أن تكون المعلومات قابلة لتحديد الهوية الشخصية ويمكن أن تكشف عن أجزاء حساسة من المعلومات مثل المعتقدات السياسية للشخص أو ميوله الجنسي أو معتقداته الدينية أو المسائل الطبية. وتستخدم هذه المعلومات بصورة عامة في أغراض التسويق، ولكن ثمة بعض المخاطر التي تكمن في الكشف عن هذه المعلومات، مثل ما نشرته شركة إيه أو إل (AOL) من معلومات في العام 2006 (كما سبق وناقشناه). وتزداد مخاطر الخصوصية وحقوق الإنسان الأخرى بشكل أكبر في الدول التي تقل فيها حماية حقوق الإنسان. ونناقش هذا الأمر بمزيد من التفصيل في القسم التالي.

---

48 EPIC، "الحوسبة السحابية" نشر على الإنترنت /http://epic.org/privacy/cloudcomputing

49 المرجع السابق

50 المرجع السابق

2. استعراض عالمي لتحديات وفرص حماية الخصوصية على الإنترنت

2.1. المسائل الأساسية

1.1.2. فرص وتحديات المراقبة المستمرة للبيانات الشخصية على الإنترنت

> «لا ينبغي أن يتعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته. ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات". هذا ما نصت عليه المادة 12 من الإعلان العالمي لحقوق الإنسان.

لقد ظلت حماية الخصوصية مكفولة كحق من حقوق الإنسان. ولكن مع التطورات التقنية الجديدة في العقود الأخيرة، ولا سيما في تقنيات المعلومات والاتصالات، واجه هذا الحق الكثير من التحديات. واستجابة لهذه الصعاب صدرت سلسلة من قوانين حماية الخصوصية في أجزاء مختلفة من العالم في العقد الثامن من القرن الماضي بهدف صون البيانات الشخصية للأفراد. وعلى الرغم من ذلك واجهت التشريعات والسياسة العامة الكثير من المشكلات في مواكبتها بشكل متزايد مع دورات التطور التكنولوجي قصيرة الأمد. وتجلت هذه المشكلة على الإنترنت عندما بات من غير المؤكد تماماً مدى مراعاة حكم الاتحاد الأوروبي الذي ينص على أنه " لكل شخص الحق في حماية البيانات الشخصية المتعلقة به أو بها".[51] هل يمتلك المستخدم الفردي للإنترنت القدرة على مراقبة بياناته الشخصية، بما في ذلك طريقة جمعها والاحتفاظ بها ومعالجتها واستخدامها والكشف عنها؟

من الناحية العملية، تظهر الكثير من سمات الإنترنت أنه من الصعب أن يتحكم المستخدم الفردي في بياناته الشخصية. حيث إن كون الإنترنت عابر للحدود يجعل من الصعب، بل وفي بعض الأحيان من المستحيل، معرفة الدول والولايات القانونية والمناطق التي ترسل إليها البيانات. وبلغت سرعة وانتشار الاتصالات عبر الإنترنت درجة يمكن معها نشر البيانات أبعد بكثير من نطاق سيطرة الفرد في أقل من ثانية. فضلاً عن ذلك، هناك سوق قوية على الإنترنت للبيانات الشخصية تتحكم فيها نماذج العمل القائمة على التسويق ويقوم المستخدمون فيها بالسداد من خلال بياناتهم وليس من خلال الأموال النقدية. وفي الوقت ذاته تتميز تكلفة هذه البيانات بأنها منخفضة للغاية مما يؤدي إلى تبادل عشرات الآلاف من سجلات بيانات المستخدم الشخصية بأقل تكلفة تذكر. وتسمح التطورات في تكنولوجيا المعالجة الحاسوبية إلى زيادة القدرة على معالجة قدر أكبر من البيانات الشخصية. وتزداد هذه العملية تعقيداً عند استخدام أطراف كثيرة مختلفة لعرض صفحة إنترنت على شاشة المستخدم. كما إن زيادة ترابط الأجهزة المتصلة بالإنترنت يجعل من الصعب وبشكل خاص التحكم في البيانات الشخصية. وأخيراً، اعتاد الكثير من مستخدمي الإنترنت على النقر على زر

---

51 المادة 8.1، ميثاق الحقوق الأساسية للاتحاد الأوروبي، 2000.

«قبول» والموافقة على تقديم بياناتهم الشخصية دون أن يبذلوا أي وقت يذكر في قراءة شروط الخدمة أو سياسة الخصوصية بالموقع الذي يدخلون عليه.

لقد أدى التوتر بين الحقوق والقدرة الفعلية لمستخدمي الإنترنت على التحكم في بياناتهم الشخصية إلى كثير من الجدل حول الخصوصية على الإنترنت. ويركز هذا الجدل في العادة على عدم قدرة المستخدم على التحكم وتمكينه من أن يقرر كيفية استخدام بياناته ومعالجتها، مع التركيز على دور المؤسسات في مراقبة وإدارة البيانات الشخصية. فضلاً عن ذلك، دائماً تكون سيطرة الجهات الخاصة في مقارنة سيطرة الجهات العامة، والتي تعتبر غير قادرة أو غير راغبة في تنفيذ الحماية الفعلية لبيانات المستخدم الشخصية.

يمكن فهم قواعد البيانات هذه في سياق العديد من المسائل الأساسية. أولها وأهمها مسألة موافقة المستخدم عن علم وكيفية الحصول عليها وضمانها وحتى إبطالها. ثانياً، مسألة الشفافية و"سهولة القراءة" التي لابد أن تتميز بها سياسات الخصوصية للمستخدم. ثالثاً، قدرة المستخدمين والجهات الخاصة على القيام باختياراتهم الفردية بشأن استخدام البيانات الشخصية على الإنترنت. حتى عندما يتفق معظم المستخدمين والجهات الخاصة والهيئات العامة، يتجاوز انتشار البيانات الشخصية قدرة أي فرد على السيطرة عليها (انظر أدناه لمزيد من التفصيل).

رابعاً، قد تتعارض حقوق الأشخاص في السيطرة على بياناتهم الشخصية مع الحقوق الأخرى مثل حق الغير في حرية التعبير، وكما هو موضح في المربع أدناه بعنوان الخصوصية المرئية و إديسون تشين (Visual Privacy and Edison Chen) ثمة تناقضات متكررة بين التقارير الإعلامية بشأن الشخصيات العامة وحقوقهم في التحكم في بياناتهم الشخصية. خامساً، مازال الدور الإشكالي لمراقبة الإنترنت من جانب السلطات العامة أمراً صعباً. وأخيراً، تمثل ملائمة عدم ذكر الهوية واستخدام الأسماء المستعارة مكوناً مهماً في الجدل العام بشأن حماية الخصوصية على الإنترنت. في حين ترتبط كل هذه المسائل بشكل وثيق بخصوصية المعلومات، فهي تقدم جواباً على تحدٍ أكبر: ما هي طبيعة الإنترنت الذي نأمل في إنشاءه؟ قد يساعد في فهم طريقة تحقيق ذلك معرفة ما تشير إليه 'النون' في "نأمل" من مجموعات معنية ودول قومية وتجمعات من الفاعلين، مع الأخذ في الاعتبار الرؤية المشتركة التي يكون عليها الإنترنت في المستقبل. إن الإجابة الموضوعية على هذا السؤال ستشكل الأساس الذي تقوم عليه الإنترنت على مستوى العالم.

1) الخصوصية المرئية وإديسون تشين (Visual privacy and Edison Chen)

كان إديسون كون-هي تشين (Edison Koon-Hei Chen) أحد كبار الممثلين في مدينة هونج كونج. وشارك في الكثير من الأفلام الإقليمية والدولية واعتبر واحداً من النجوم الساطعة في سماء المنطقة، وله أعمال في هوليوود مثل الليلة المظلمة (The Dark Night). وفي يناير/ كانون الثاني من عام 2008 بدأ ظهور صور جنسية لشين مع نساء أخريات من السينما في الصين على الإنترنت وانتشرت بشكل كبير في وسائط الإعلام الرئيسية. وعلى الرغم من تدخل سلطات الشرطة القومية والدولية لمحاولة وقف انتشار هذه الصور، إلا أنهم على ما يبدو عجزوا عن ذلك[52] واستمر انتشار هذه الصور عبر الإنترنت نظراً لأن اسم الممثل كان من بين أكثر الكلمات بحثاً على الإنترنت في الصين

52 بانغ دي، وتشين بي و لي دي (2008) (Pang, D., Chen, B., & Lee, D.). ثمانية محتجزون قيد التحقيق في قضية جنس على الإنترنت. The Standard. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011. من http://www.thestandard.com.hk/news_detail.asp?pp_cat=12&art_id=61125&sid=17431562&con_type=3#.

في العام 2008.[53] وقد أدين تقني الكمبيوتر الذي قام بإصلاح الكمبيوتر المحمول لإديسون تشين بسرقة الصور عند إصلاحه للجهاز في العام 2007.[54] وبمجرد ظهور الصور على الإنترنت، أصبح من الصعب إن لم يكن من المستحيل، وقفها أو مسحها. وفي هذا السياق كان الانتشار الواسع للصور مدفوعاً برغبة الجمهور العارمة في الحصول عليها. فكان إعادة نسخ هذه الصور وطلبها بكل وضوح بمثابة انتهاك للخصوصية الشخصية والطلب العام الشديد على مثل هذه الصور، وهو ما أثار تساؤلات حول كيفية تعزيز ثقافة خصوصية المعلومات.

2.1.2. مبادرات حماية الخصوصية وسرية الهوية على الإنترنت

استجابة للكثير من هذه التساؤلات أطلقت مجموعة متنوعة من المبادرات على الإنترنت لحماية خصوصية الأفراد. وهنا تكمن أهمية كبيرة في قيام المجتمع المدني بإطلاق وتنظيم مبادرات تهدف إلى حماية الخصوصية وسرية الهوية على الإنترنت.

وينعكس هذا الدور في العديد من المبادرات المهمة التي يتولى زمامها المجتمع المدني. وفي هذا الإطار، كان من أهم المبادرات تلك التي تهدف إلى زيادة الوعي لدى المستخدمين وتثقيفهم بشأن أهمية خصوصيتهم وكيفية حمايتها. ومن الأمثلة على ذلك مشروع 'الدفاع عن النفس ضد المراقبة' الذي أنشأته مؤسسة Electronic Frontier Foundation، ومشروع 'Big Brother Inc' الذي يصنف الشركات القائمة باستيراد تقنيات المراقبة ومشروع 'Me and my own Shadow' الذي هو عبارة عن حملة توعية بمبادرة من المؤسسة غير الحكومة TacticalTech.

2) مبادرة المواطنين بشأن الاحتفاظ بالبيانات

من أهم مبادرات المستخدم لحماية الخصوصية وسرية الهوية على الإنترنت مبادرة المواطنين الألمان بشأن الاحتفاظ بالبيانات. حيث قام ما يزيد على 34,000 مواطن برفع دعوى دستورية جماعية ضد قانون الاحتفاظ بالبيانات الذي تم تمريره قبل ذلك بقليل لدى المحكمة الدستورية الألمانية في عام 2007.[55] ويمثل هذا العمل الجماعي أكبر قضية مشتركة في تاريخ المحكمة الدستورية الألمانية. واستغرق الأمر عدة أشهر لقيام المحامين بالحصول على التوقيعات وتقديمها إلى المحكمة. أصدرت المحكمة الدستورية أمراً مبدئياً ضد قانون الاحتفاظ بالبيانات في العام 2008، ثم أعلنت عدم دستورية القانون في العام 2010.[56] ونظراً لأن المحكمة الدستورية الألمانية لم تقبل سوى عدداً قليلاً جداً من الدعاوي الدستورية المرفوعة لديها، وأن 1–2% منها كان صحيحاً، فقد كانت هذه الدعوى المشتركة الناجحة بمثابة لحظة تاريخية. لذا نجحت المبادرة ليس فقط في إعلان عدم دستورية قانون الاحتفاظ بالبيانات، ولكن أيضاً في وضع الخصوصية وسرية الهوية في مقدمة الرأي العام في ألمانيا. ونظراً لأن قانون الاحتفاظ بالبيانات الألماني كان عبارة عن ترجمة لتوجيه صادراً عن الاتحاد

53 Google. (2008). Google Zeitgeist 2008. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011 من https://www.google.com/intl/en/press/zeitgeist2008/world.html#top

54 بومفريت جي (Pomfret, J) (2009). فني يتهم بالتورط في سرقة صور الجنس الخاصة بإديسون تشين. Victoria News. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011 http://www.vicnews.com/entertainment/television/43998412.html

55 Initiative Vorratsdatenspeicherung. (2011). Stoppt die Vorratsdatenspeicherung. تم الاسترجاع في 13 نوفمبر/ تشرين الثاني 2011 https://www.vorratsdatenspeicherung.de/static/verfassungsbeschwerde_de.html.

56 BVerfG, 1 BvR 256/08 بتاريخ 2.3.2010, الفقرة– 345 – 1) .Nr), http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html.

الأوروبي خرج في النهاية في صورة قانون من القوانين الألمانية القومية، فقد تردد صدى هذا القرار خارج حدود ألمانيا وكان له أثر عظيم على مناقشة وممارسة الاحتفاظ بالبيانات في أوروبا كلها.

تظهر هذه المشاريع الدور الحيوي الذي يمكن للمجتمع المدني أن يلعبه في زيادة التوعية بمسائل الخصوصية وتزويد المستخدمين بالمصادر اللازمة للدفاع عن خصوصيتهم وتثقيف المواطنين بشأن أنشطة صناعة المراقبة. ولعبت منظمات المجتمع المدني على المستويين الدولي والمحلي دوراً أساسياً في هذا السياق في تمكين المستخدمين بالتكنولوجيا لتنفيذ اختيارات مستنيرة بشأن بياناتهم الشخصية.

كما إن المبادرات الفنية لها دور قيم في حماية الخصوصية وسرية الهوية على الإنترنت. فلقد ساهم تطور أدوات المصادر المتاحة لمستخدمي الإنترنت مثل Tor أو GnuPG أو HTTPSEverywhere بشكل كبير في خصوصية وسرية هوية المستخدمين على الإنترنت. حيث توفر هذه البرامج المتاحة لمستخدمي الإنترنت مستوى أكبر من سرية الهوية وتسمح لهم بتأمين ملفاتهم ورسائلهم الالكترونية وتوفر قدراً أكبر من الأمن عند الدخول على الكثير من المواقع الالكترونية.

ولقد تلقت كل هذه الجهود الفنية دعماً وتطويراً مكثفاً من مستخدمي الإنترنت حول العالم والعديد من منظمات القطاع المدني. ومن الجدير بالذكر أن معظم المبادرات الخاصة تركز على تزويد المستخدم النهائي بالقدرة على الحصول على تقنيات تشفير قوية تكون بمثابة قوة موازنة قيمة لتقنيات مراقبة الإنترنت. ولقد ذكر مراراً وتكراراً من جانب الخبراء الأكاديميين والفنيين وكذلك المجتمع المدني بأن التوسع الهائل في استخدام تقنيات التشفير القوية بين مستخدمي الإنترنت سيكون له تأثير إيجابي جداً على الخصوصية وسرية الهوية على الإنترنت.

3) مبادرات الشركات الداعمة لحرية التعبير والخصوصية: مبادرة Global Network

فضلاً عن مبادرات المواطنين، فإن واحدة من أبرز المبادرات التي تتميز بالتنظيم الذاتي بين مؤسسات الإنترنت هي مبادرة الشبكة العالمية (GNI). حيث تجمع بين شركات التكنولوجيا والمنظمات غير الحكومية والمؤسسات الأكاديمية. وعلى الرغم من نجاح هذه المبادرة في زيادة الوعي بدور الشركات في حماية ودعم حقوق الخصوصية وحرية التعبير، إلا إن عدد الشركات الأعضاء فيها لا يزال محدوداً، مع عدد قليل من الشركات الكبرى: جوجل (Google) وياهو (Yahoo) وميكروسوفت (Microsoft).

وعلى الرغم من أن الكثير من شركات الإنترنت الأخرى قد طلب منها و/أو تم دعوتها للانضمام إلى هذه المبادرة، إلا أن معظم هذه الدعوات لم تنجح. ونظراً لأن هذه المبادرة لم يمضي على إطلاقها فترة طويلة، فما زلنا نرى كيفية تأثير متطلبات التقرير الخاصة بها على ممارسات الشركات الفعلية على المدى المتوسط والبعيد.

فضلاً عن مبادرات المجتمع المدني، لعبت كذلك مبادرات المستخدم هي الأخرى دوراً مهماً في حماية الخصوصية وسرية الهوية على الإنترنت. وعادة ما تركز مبادرات المستخدمين على مسألة واحدة محددة، بدلاً من مفهوم الخصوصية ككل. ومن الأمثلة العديدة المهمة على مبادرات المستخدم الرامية لحماية الخصوصية وسرية الهوية على الإنترنت تلك الحملات التي أطلقت من أجل التغييرات على «سياسات الاسم الحقيقي» من جانب مستخدمي الشبكات الاجتماعية وزيادة الوعي بمخاطر مشاركة البيانات الشخصية على الإنترنت

والدعوى القضائية التي ضمت ما يزيد على 30 ألف فرد لدى المحكمة العليا الألمانية للطعن في دستورية قوانين الاحتفاظ بالبيانات.

والجدير بالذكر أيضاً أن هناك مبادرات من شركات لحماية الخصوصية من بينها مبادرة الشبكة العالمية (GNI) التي تعتبر أشهرها (أنظر المربع أعلاه). وعلى الرغم من ذلك، ثمة الكثير من الجدل حول فعالية التنظيم الذاتي للمؤسسات على الإنترنت. وفيما يتعلق خصيصاً بالخصوصية، يقال في كثير من الأحيان أن أرباح الشركات تتأتى من بيع بيانات عملائها وليس لديها أي مصلحة في تقديم أي شيء يتعدى مشاريع مسؤولية الشركة الاجتماعية "التي يتسترون بها" لإخفاء دوافعهم الحقيقية. وإن الاستجابة الأكثر شيوعاً لهذه المطالبة هو أن الشركات تحتاج إلى ثقة المستخدم وأي خرق جسيم لثقتهم قد يضر بالشركة المخلة بهذه الثقة. وفي أي من الحالتين، ثمة حوافز متضاربة بشكل واضح للشركات المشاركة في هذه المبادرات وليس من المؤكد مدى استطاعة أنظمة الخصوصية ذات التنظيم الذاتي لتحل محل التشريعات واللوائح العامة.

وأخيراً، توجد عدم ثقة ملحوظة لدى العديد من مناصري الخصوصية وعدم الكشف عن الهوية في فعالية الحلول التنظيمية والقضائية والحكومية، وثمة خوف واسع بأن تأتي التنظيمات العامة للخصوصية بتأثيرات عكسية بسبب المصالح الخاصة أو تقوم على أساس معلومات غير صحيحة أو غير فعالة. وفي حين استمرار مطالبة المناصرين بالتغيير التنظيمي على مسائل الخصوصية ومواصلة التماسهم لسبل الانصاف ضد انتهاكات الخصوصية باللجوء إلى النظام القضائي، هناك تركيز قوي على تمكين المستخدمين من التأكد من عدم اعتمادهم على الأنظمة العامة. حيث يركز هذا النهج على تزويد المستخدمين بالأدوات الضرورية لحماية خصوصيتهم وزيادة مستوى الوعي بقضايا الخصوصية. وتقترح الإستراتيجية الرئيسية لتمكين المستخدمين النهائيين من حماية خصوصيتهم إلى عدم اقتناع الكثير من المناصرين بقدرة أو رغبة الدول في معالجة بعض قضايا الخصوصية الأكثر تعقيداً.

3.1.2. أدوار ومسؤوليات مزودي الخدمة والوسطاء

يلعب مزودو خدمات الإنترنت ووسطاء الإنترنت دوراً بالغ الأهمية على شبكة الإنترنت، ويتجاوز دورهم الدور المعتاد لأي شركة تقدم منتجاً قياسياً في السوق التقليدية. ولأن مقدمي خدمات الإنترنت ووسطاء الإنترنت يتعاملون بالمعلومات، تكون هذه الشركات قادرة بأعمالها على حماية العديد من الحقوق والحريات الخاصة بالمستخدمين على شبكة الإنترنت أو ضياعها. وعلاوة على ذلك، لا يأتي هذا الدور المهم من فراغ السلطة وترتيبات الإدارة الوطنية والدولية المختلفة، بل إن المصالح السياسية والتجارية غالباً ما تتعارض بغرض بسط سيطرة أكبر على وسطاء الإنترنت. ومن ثم لا يمثل حماية هذه الشركات من 'مسؤولية الوسيطة' أمراً بديهياً، بل هي صفقة سياسية معينة تواجه المزيد من التحديات المستمرة في سياقات مختلفة.[57] واستجابة لهذه المطالب أصدر مناصرو حقوق الإنسان دفاعات قوية تستوجب دراسة قواعد مسؤولية الوسطاء وفقا لمعايير الحماية الدولية.[58]

ولكن في كثير من الحالات توجد آليات أخرى يتم من خلالها إجبار الوسطاء على التعدي على خصوصية مستخدميهم من غير المسؤولية القانونية وحدها. خاصة وأنه يتعرض مزودو خدمة الإنترنت (ISP) إلى الإجبار بشكل متكرر للقيام "بالمراقبة الطوعية" لتحركات مستخدميهم، مما ينتج عنه خلق بنية تحتية ومؤسسات تقوم بجمع ومعالجة البيانات الشخصية للمستخدم بما يتجاوز أي آليات لازمة لتوفير خدمات الإنترنت،

---

57 مويلر (2010) (Mueller) الشبكات والدول، مويلر، إم. إل. (2010) (.Mueller, M. L) الشبكات والدول: السياسة العالمية لإدارة الإنترنت، ص. 138–139. مطبعة MIT Press

58 لا ريو إف (2011) (.La Rue, F)، تقرير المقرر الخاص بشأن دعم وحماية الحق في حرية الرأي والتعبير، فرانك لا ريو (Frank La Rue) إلى مجلس حقوق الإنسان لدى الأمم المتحدة [23/A/HRC/14]. جنيف: الأمم المتحدة.

وهذا مجرد مثال واحد من أمثلة كثيرة يتم فيها إجبار الوسطاء على تحقيق رغبات أطراف ثالثة للتعدي على خصوصية المستخدم أو تقييدها.

وفي نفس الوقت كلما كانت أعمال وسطاء الإنترنت عابرة للحدود الوطنية ومنفصلة عن أي موقع مادي، كلما زادت المرونة التي يحصلون عليها في تعاملاتهم مع السلطات التشريعية. وهنا يلعب الوسطاء العابرون للحدود الوطنية دوراً كبيراً في هذا السياق، أمثال شركة جوجل (Google) أو مايكروسوفت (Microsoft) أو الفيسبوك (Facebook) أو أمازون (Amazon) الذين يمكنهم التفاوض مع الدول القومية على شروط تبدو متكافئة على أساس حجمها ونطاقها الدولي. كما يعطيهم بيعهم للبرامج أو الخدمات الالكترونية في الأساس مستوى كبير من المرونة فيما يتعلق بمواقعها الفعلية. والنتيجة هي القدرة على "انتقاء واختيار" الولايات القضائية.

وتتنافس الدول القومية في جميع أنحاء العالم على استضافة الشركات، وثمة مؤشرات عديدة تم التوصل إليها من خلال عملية البحث تفيد بأن العديد من البلدان قد اختارت أنظمة خصوصية ضعيفة من الناحية الإستراتيجية، وذلك لتحقيق ميزة تنافسية (مفترضة) نحو الاقتصادات المتقدمة الأخرى. وتتم هذه الخيارات الإستراتيجية في كثير من الحالات من قبل الدول الصغيرة التي اختارت أن تصبح محاور إقليمية لصناعة التكنولوجيا المتقدمة. ويبدو أن هذه المنافسة للتأكيد على منافسة سياسة الخصوصية بين البلدان والتي تُدعم على الأقل بشكل غير مباشر عن طريق الشركات عبر الدولية.

ومن المسائل الأخرى التي أصبحت محل جدل بالغ من منظور الخصوصية هي تشريعات الاحتفاظ بالبيانات التي من خلالها يتواطأ مزودو خدمة الإنترنت في مراقبة وتخزين ممارسات عملائهم على الإنترنت على نطاق واسع. وتتم هذه التدابير عادة على نطاق واسع دون أي دليل على اقتراف عملاء مزودي خدمة الإنترنت (ISP) الخاضعين للمراقبة لأي جريمة. ومع ذلك يدعي الكثير بأن هذه التدابير يمكن أن تساعد في التحقيق في الجرائم التي ارتكبت على شبكة الإنترنت. وثمة إشكالية أخرى وهي حماية الأطفال (انظر المربع لمزيد من التفاصيل) وتنفيذ حق المؤلف، حيث تعرض مزودو خدمة الإنترنت ووسطاء الإنترنت إلى ضغط كبير للتدخل في خصوصية عملائهم[59] بطرق لا ترقى إلى مبادئ الحماية مثل الشفافية ومراعاة الأصول القانونية والمساءلة.

كما أنه يمكن للضغط على وسطاء الإنترنت، مثل جوجل (Google) أو الفيسبوك (Facebook) أو أمازون (Amazon)، أن يسبب آثاراً سلبية كبيرة على الخصوصية على الإنترنت. فعلى عكس التفاعلات غير المتصلة بالإنترنت التي يصعب للغاية فيها رؤية التفاعلات الشخصية والاقتصادية والسياسية على نطاق واسع، فإن التفاعلات عبر الإنترنت تترك «أثراً للبيانات». ولقد بدأت شركة جوجل (Google) في الاستجابة لهذه الضغوط من خلال نشر «تقارير الشفافية» بشكل دوري بهدف توعية المستخدمين حول مدى طلب الحكومات للبيانات المتعلقة بهم. وفي حين أن هذا بمثابة خطوة أولية قيمة، فإنها لا تكفي لتعيين العديد من التفاعلات القسرية غير الرسمية التي تجري من أجل الحصول على البيانات الخاصة من الشركات الخاصة، أو للوقوف على سبب طلب هذه البيانات.

لعب مزودو خدمة الإنترنت (ISP) المملوكة للدولة دوراً معقداً بشكل خاص في هذا السياق، حيث إن ملكيتها للدولة وسيطرتها النموذجية على الكثير من البنية التحتية الأساسية للإنترنت يجعلها أقل استقلالية عن الدولة. وهذا قد يكون له غالبا أثر ضار على خصوصية المستخدمين، لا سيما في البلدان التي لا تقدم الاهتمام اللازم للخصوصية، و لحقوق الإنسان بشكل عام لمستخدمي الإنترنت. وعلى العكس من ذلك، من المرجح أن توفر خصخصة مزودي خدمة الإنترنت (ISP) المملوكين للدولة إلى جانب فصل الحلقات المحلية (LLU) هيكل

59 مويلر (2010) (Mueller) الشبكات والدول، مويلر، إم. إل. (2010) (Mueller, M. L.) الشبكات والدول: السياسة العالمية لإدارة الإنترنت، ص 150–151. مطبعة MIT Press

سوق لمزودي خدمات الإنترنت (ISP) من شأنه أن يوفر مزيداً من حماية الخصوصية. وثمة سياسات محددة مثل خصخصة مزودي خدمات الإنترنت (ISP) المملوكين للدولة وفصل الحلقات المحلية (LLU) قد ينتج عنها سوق تنافسية وقوية لمزودي خدمات الإنترنت. وحتى يعمل سوق مزودي خدمات الإنترنت على النحو الملائم لابد أن يساهم بدوره في حماية خصوصية المستخدمين عن طريق منع أسواق الاحتكار أو احتكار القلة التي لا يوجد فيها سوى عدد قليل من نقاط التحكم.

وبصورة أعم، يواجه مزودو خدمة الإنترنت (ISP) موقف صعب بشكل خاص لمقاومة التعدي على خصوصية مستخدميهم لخضوعهم عادة لاتفاقات الترخيص التي تشترط عليهم تقديم بيانات إلى الهيئات العامة. وفي حين أن هذا قد يكون مشروعاً تماماً في بعض الحالات، إلا إنه يضعهم في وضع سيئ بالنسبة لوسطاء الإنترنت الآخرين الذين هم أقل عرضة للإكراه على تقديم بيانات المستخدم. إن تطور نموذج أعمال مزودي خدمة الإنترنت (ISP) إلى تقديم خدمات ومحتوى إضافي في صورة حزم لمستخدمي الإنترنت يعني أن مزودي خدمة الإنترنت (ISP) أصبحوا عرضة للإكراه التنظيمي أكثر من أي وقت مضى.

ويزيد هذا التطور كثيراً من خلال ما يمكن توفيره من جانب مزودي خدمة حزم الإنترنت الإضافية، مع إخضاعهم للشروط التعاقدية لأصحاب حقوق التأليف والنشر الذين يشترطون على مزودي خدمة الإنترنت التعدي على خصوصية مستخدميهم مقابل وصولهم إلى محتوى الإنترنت الإضافي. ويرحب بهذا التطور بعض من مزودي خدمة الإنترنت في قطاع الاتصالات المتنقلة، وذلك لامتلاكهم بنية إنترنت تحتية ذات خصوصية محدودة، وبالتالي تمتعهم بـــ «ميزة المتحرك الأول" على غيرهم من مزودي خدمة الإنترنت عند تقديم بيانات مستخدميهم إلى من يتعاقدون معهم. وكما أشار ممثل لأحد مزودي خدمات الإنترنت خلال مقابلة معه، يتطلب الأمر عزيمة كبيرة لمقاومة المطالب المتكررة للحصول على بيانات المستخدم الخاصة من جانب السلطات الرسمية بالدولة.

وبصورة أعم، لقد صعبت ترتيبات الإدارة على المستويين الوطني وعبر الدولي من وقف التبادل الدولي لبيانات الأفراد الشخصية والتي تتعدى على الخصوصية بكل معانيها، أو لتوفير سبل انصاف فعالة للانتهاكات الخصوصية عبر الحدود. ويلعب الوسطاء عبر الدوليين أدواراً مختلفة عادة في هذه المبادرات، وربما لا يلتزمون دائماً بنهج قائم على أساس الحقوق في الخصوصية. ومن أكبر التحديات أمام صون حقوق الإنسان في مجتمع المعلومات العالمي هو إيجاد آليات إدارة فعالة لحماية البيانات والخصوصية.

4) خصوصية الأطفال والشباب

تحتم المخاوف المتعلقة بالخصوصية إيجاد طرق مختلفة من التفكير لأفراد مختلفين.[60] ففي دراسة حديثة، اقترحت وكالة أمن المعلومات والشبكات الأوروبية (ENISA) أن حماية خصوصية الشباب هي إحدى الاستراتيجيات الرئيسية لمكافحة التعدي الالكتروني والاستمالة على الإنترنت.[61] حيث يقومون بتحديد منصات إنترنت مصممة بشكل غير صحيح ومستويات عالية إلى درجة غير ضرورية من التعقيد فضلاً عن قلة الوعي كنقطة ضعف رئيسية بشأن خصوصية الشباب على الإنترنت. ونتيجة لذلك، فإن واحدة من أهم توصيات وكالة أمن المعلومات والشبكات الأوروبية (ENISA) هي «عدم إتاحة إمكانية إنشاء واستخدام ملفات التعريف لمن هم دون السن القانونية بشكل عام»[62]وفرض

---

60 Hilles, L., & Jugendschutz.Net. (2011). Verlockt – Verlinkt – verlernt? Werbung, Vernetzung und Datenabfragen auf Kinderseiten. Mainz, Germany.

61 مارينوس، إل (Marinos, L.) ووكالة أمن المعلومات والشبكات الأوروبية (2011). التعدي الالكتروني والاستمالة الالكترونية: المساعدة في الحماية من الأخطار. إيراكليو، ألمانيا.

62 المرجع السابق، صفحة 47.

عقوبات مالية أشد على الشركات التي تخرق هذه القوانين. ففي الولايات المتحدة الأمريكية، تم وضع قانون حماية خصوصية الأطفال على الإنترنت لضمان حصول مواقع الإنترنت على موافقة الآباء قبل جمع البيانات الخاصة بكل من هو دون سن 13 سنة. ونتيجة لذلك، تختار العديد من مواقع الإنترنت مثل فيسبوك (Facebook) استبعاد الأفراد دون سن 13 من موقعها الإلكتروني. وفي نفس الوقت، تشير الأبحاث الأكاديمية إلى أن كثير من الآباء يساعدون أطفالهم في التحايل على قيود السن للوصول إلى موقع فيسبوك (Facebook)[63]، مما يثير تساؤلات واضحة حول قدرة التشريعات الحالية على حماية خصوصية الأطفال والشباب على الإنترنت.

2.2. تحديات محددة تمثلها التطبيقات ومنصات الاتصالات ونماذج الأعمال المختلفة

1.2.2. الحوسبة السحابية

الحوسبة السحابية هي تطور حديث نسبياً يمكن من تخزين كميات متزايدة من البيانات – بما فيها البيانات الشخصية – في "سحابة" على الإنترنت، وعند التخزين يتم نقل البيانات الشخصية عبر الإنترنت، مما قد يشكل خطراً حقيقياً على مدى قدرة الفرد على التحكم في تلك البيانات. وبمجرد تخزين البيانات في السحابة، تستمر هذه المخاطر، حيث يمكن على سبيل المثال "لمزود السحابة، ودون إشعار المستخدم، نقل معلومات المستخدم من مكان إلى آخر، ومن مزود إلى مزود آخر أو من جهاز إلى آخر."[64]

وعلاوة على ذلك، قد تتعرض بيانات المستخدمين الشخصية في السحابة لتغييرات ديناميكية من حيث الخدمة، حيث "من الشائع أن تحتفظ أي شركة إنترنت تقوم بوضع شروط الخدمة أو سياسة الخصوصية بالحق في تغيير تلك الشروط أو تلك السياسة دون قيد".[65] وهذا التحذير المهم يعني أنه يمكن في كثير من الحالات تغيير سياسة الخصوصية أو «شرط من شروط الخدمة» التي تعتبر صارمة لحماية البيانات من يوم إلى آخر. وتقتصر قدرة المستخدمين على الاستجابة لهذه التغيرات، وفي بعض الحالات لا يعلمون بها أو يعجزون عن فهم الآثار المترتبة عليها بخصوص البيانات الشخصية الخاصة بهم.

وتتقابل حماية البيانات الشخصية مع النموذج التجاري من الحوسبة السحابية نفسها، والذي بطبيعته يتوقع قيام المستخدمين (الذين هم عملاء لهم في كثير من الحالات) بنقل بياناتهم الشخصية على الإنترنت، وبذلك يقوم المستخدمون في العادة بالتنازل عن «سيادة البيانات»، أي لن يكونوا قادرين على تحديد المنقطة المحددة التي توجد فيها بياناتهم الشخصية. فضلاً عن ذلك، يمكن للتحكم المركزي في هذه البيانات من قبل مزود السحابة أن يخضع هذه البيانات إلى خوارزميات حاسوبية تكشف عن معلومات شخصية لم يرغب المستخدمون في الإفصاح عنها أو لم يكونوا على علم بها، كما تترك بياناتهم الشخصية متاحة للارتباط من قبل مزود السحابة وربطها بقواعد بيانات طرف ثالث. وقد تتعرض البيانات المخزنة في السحابة أيضاً إلى أمر قضائي أو مذكرة استدعاء أو تحقيق في أي ولاية قضائية يقوم فيها مزود السحابة بتعيين موظفين أو امتلاك أصول. وبالنسبة للشركات الكبيرة، ولا سيما الشركات العابرة للحدود الدولية والتي تعمل في

---

63 (Facebook) لماذا يساعد الآباء أطفالهم في التحايل على الفيسبوك.
(2010) Boyd, D., Hargittai, E., Schultz, J., & Palfrey, J. 63

64 جيلمان، آر (.Gellman, R)، ومندى الخصوصية العالمي. (2009). الخصوصية في السحب: مخاطر تتعرض لها الخصوصية والسرية ناتجة عن الحوسبة السحابية. تم الاسترجاع من:
.http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

65 المرجع السابق.

تزويد السحابات، يتوقع زيادة عدد الحكومات القادرة على أن تطلب الاطلاع على البيانات المخزنة في السحابة بشكل كبير.

يمكن معالجة العديد من هذه المسائل من خلال توفير التشفير القوي لمستخدمي الخدمات المقدمة في السحابة، سواء عند نقل البيانات أو بعد تخزينها. حيث إن هذه التدابير من شأنها ضمان وصول المستخدم فقط إلى بياناته الشخصية. ولكن في الوقت الحاضر لا يقدم هذا المستوى من التشفير القوي للبيانات سوى عدد قليل جداً من مزودي السحابات – سواء عند نقل البيانات أو بعد تخزينها، وفي نفس الوقت ثمة جدل جاري في أوساط مجتمع الإنترنت حول مدى الثقة بمزودي السحابات. فمع استمرار تخزين بعض أكبر مزودي خدمات البريد الإلكتروني لتخزين المعلومات الشخصية في السحابة دون تشفيرها، فلا يبدو أن شكوك مجتمع الإنترنت لا أساس لها. بل تؤكد هذه الشكوك عند اختراق خدمات الإنترنت في السحابة والكشف عن كميات هائلة من البيانات (انظر المربع أدناه لمزيد من التفاصيل).

5) فقدان 85% من البيانات الشخصية لمستخدمي الإنترنت في جمهورية كوريا

في منتصف عام 2011 تعرض مواطنو جمهورية كوريا إلى أكبر خسارة للبيانات الشخصية في تاريخ البلاد، عندما أعلنت شركة اتصالات كوريا الجنوبية (SK Communications Co.) للجمهور عن اختراق المعلومات الشخصية الخاصة بـــ 35 مليون عميل، وسرقة البيانات الشخصية خاصة من موقع التواصل الاجتماعي Cyworld ومحرك البحث Nate الخاص بالشركة، وهما من أكبر المواقع في جمهورية كوريا. وكان من بين المعلومات الشخصية أسماء المستخدمين وكلمات السر وأرقام الضمان الاجتماعي وأرقام تسجيل المقيمين وأرقام الهواتف المحمولة وعناوين البريد الإلكتروني والصور الشخصية.[66] ووفقاً للاتحاد الدولي للاتصالات السلكية واللاسلكية (ITU) أنه قد سرقت المعلومات الشخصية لما يقرب من 40 مليون مستخدم للإنترنت في جمهورية كوريا، أي أكثر من 70% من السكان الكوريين أو تقريبا 90% من مجموع مستخدمي الإنترنت في جمهورية كوريا.[67] وقبل الهجوم كانت حكومة جمهورية كوريا تطبق سياسة «الاسم الحقيقي»، مما اضطر المستخدمين من المواقع الكبيرة لاستخدام أسمائهم الحقيقية وتقديم رقم الضمان الاجتماعي لإثبات هويتهم، ثم أعلنت الحكومة عن ضرورة تغيير هذه السياسة بعد الهجوم، ثم ألغيت في نهاية المطاف من قبل المحكمة الدستورية الكورية في أغسطس/ آب 2012. ومع ذلك، فإن الصدمة الصارخة التي نتجت عن خرق البيانات في جمهورية كوريا هي عبارة عن قصة تحذيرية لصناعة الإنترنت أصحبت فيها سيطرة القلة على البيانات الشخصية أمراً اعتيادياً بشكل كبير.

في كثير من الحالات يتعرض مزودو خدمة الحوسبة السحابية لقرارات من جانب وسطاء الإنترنت. وبغض النظر عن درجة الحماية التي يعد بها مزود الحوسبة السحابية من حيث الخدمة، يتم في نهاية المطاف تحديد أمن وسرية المعلومات الشخصية من خلال الحلقة الأضعف في السلسلة. ومع انخراط عدة وسطاء في نقل وتخزين المعلومات الشخصية في السحابة، لا يحتاج الأمر إلا أن يفشل واحد منهم فقط إما عن قصد أو

66 سونج جين، واي (Sung-jin, Y.) (2011) اختراق معلومات 22 مليون مستخدم لــ Cyworld وNate. مجلة The Korea Herald. تم الاسترجاع في 12 ديسمبر/ كانون الأول 2011، من .
http://www.koreaherald.com/national/Detail.jsp?newsMLId=20110728000881

67 مركز بحوث الاتصالات السلكية واللاسلكية. (3313). الاتصالات السلكية واللاسلكية الدولية. جنيف: الاتحاد الدولي للاتصالات السلكية واللاسلكية.

عن غير قصد للكشف عن المعلومات الخاصة.[68] في الوقت نفسه يتعرض مزودو الحوسبة السحابية لبرامج المراقبة الحكومية، وذلك لنقلهم كميات كبيرة من البيانات الشخصية عبر شبكة الإنترنت العامة من أجل تخزينها في السحابة، وقد يستمر في كثير من الحالات في نقلها عبر شبكة الإنترنت العامة بين أجزاء مختلفة من السحابة. هذه الإجراءات تجعل من المستحيل تقريباً على المستخدم النهائي أن يقول بيقين مطلق ما هي الأقاليم التي تُنقل خلالها بياناته الشخصية. وبالتالي يصبح من الصعب جداً أيضاً على مستخدمي الحوسبة السحابية التيقن من برامج المراقبة الحكومية التي تخضع لها بياناتهم الشخصية.

وأخيراً هناك العديد من المسائل القانونية العالقة فيما يتعلق بحماية البيانات الشخصية من خلال الحوسبة السحابية. فبما أن «السحابة قد يكون لها أكثر من موقع واحد قانوني في وقت واحد، مع اختلاف الآثار القانونية المترتبة عليها»،[69] فإنه يبقى من غير الواضح كيف سيكون رد فعل مزودي السحابة في سياق محدد. والحوسبة السحابية ليست عاجزة بطبيعتها عن حماية البيانات الشخصية. بيد أن نموذج الأعمال التجارية، الذي يقوم على جمع البيانات الشخصية في منصة معالجة مركزية عبر شبكة اتصالات موزعة، سيثير تساؤلات كبيرة حول حماية البيانات الشخصية.

2.2.2. محركات البحث

لقد قدمت محركات البحث على مر السنوات الماضية وظيفة حيوية على شبكة الإنترنت من خلال مساعدة المستخدمين على التنقل بين المصادر الهائلة المتاحة على الإنترنت، مثل العديد من خدمات الإنترنت التي تقدمها بصورة مجانية، مع تركيز نموذج الأعمال التجارية على الإعلانات. وفي نماذج الأعمال هذه لا يقوم المستخدمون بدفع الأموال نقداً ولكن من خلال الإدلاء ببياناتهم ثم عرض الإعلان على أساس البيانات المقدمة. وكلما كانت البيانات الشخصية كاملة وجيدة، كلما زادت فعالية الإعلان المقدم. ومن ثم، لا يبدو من غير المعقول أن نشير إلى أن محركات البحث على شبكة الإنترنت تهدف إلى جمع البيانات الشخصية إلى أقصى حد ممكن نظراً لنموذج أعمالها.

لقد وسعت محركات البحث على الإنترنت في كثير من الأحيان من خدماتها لتشمل أنواع أخرى من الخدمات مثل البريد الإلكتروني أو مشاركة الصور التي يمكن توفيرها للمستخدمين. وتسمح هذه الخدمات الإضافية لمحركات البحث أن تربط المعلومات بإشارة مرجعية بين الخدمات المختلفة وبالتالي بناء ملفات تعريف المستخدم بمعلومات أكثر. وفي حين يسهل تأثير التكامل من استخدام الخدمات المتعددة المتكاملة ويزيد قيمتها بالنسبة للمستخدمين، فإنهم يدفعون أموالاً على نحو متزايد من خلال الإدلاء ببياناتهم الشخصية وتقديم عرض كامل تماماً عن حياتهم الشخصية. وثمة تضارب مماثل موجود بالفعل فيما يتعلق بالتخصيص، حيث يقوم مستخدمو محركات البحث بالكشف عن بعض خصوصياتهم مقابل الحصول على مزيد من مزايا تخصيص خدمات البحث. وهنا، قد تكون قيمة الخدمة مرتفعة، ولكن المستخدم ’يدفع‘ مقابل هذه الخدمة المتطورة عن طريق التضحية ببعض بياناته الشخصية.

ومن التطورات الأخرى الملحوظة ظهور ما يسمى بـ ’محركات البحث الوطنية‘ في الصين والاتحاد الروسي وأجزاء أخرى من العالم. حيث جاءت المحركات لتتحدى محركات البحث الدولية المهيمنة وحققت نجاحاً خاصاً في أجزاء محددة من العالم، ولكن ثمة قلق كبير في مجتمع الإنترنت حول ممارسات الخصوصية الخاصة بهم. فبينما تكون الجهات الفاعلة عبر الدولية على استعداد لتحدي ممارسات خصوصية المستخدم الأكثر تقييداً في أجزاء مختلفة من العالم، فإن محركات البحث الوطنية مرتبطة بأسواقها المحلية الرئيسية،

---

68 فيليب بي دو (Filippi, P. de.) (2011). ملاحظات عن الخصوصية في السحابة.

69 جيلمان، آر (Gellman, R.)، ومندى الخصوصية العالمي. (2009). الخصوصية في السحابات: مخاطر تتعرض لها الخصوصية والسرية : ناتجة عن الحوسبة السحابية. تم الاسترجاع من http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

مما يجعل محركات البحث الوطنية هذه تحت رحمة الأطر التنظيمية الوطنية في الأسواق المحلية التي ينتمون إليها. وبقدر حماية هذه المحركات للخصوصية، يمكن رؤية هذا على أنه تطور إيجابي، ولكن ليس هذا هو الحال بصورة عامة، بل يوجد في نفس الوقت دلائل على أن 'المنافسة على أساس الخصوصية' قد تكون قد بدأت ببطء بين محركات البحث. ومن خلال المستخدمين والمجتمع المدني والضغوط التنظيمية معاً، بدأت بعض محركات البحث في التوصل إلى ابتكارات في ميدان سياسات الخصوصية.[70] ويعتبر هذا مؤشر مشجع، فقد نأمل بأن تدفع المنافسة بين محركات البحث باتجاه تحسن عام في سياسات الخصوصية. ومع ذلك، ليس من الواضح ما إذا كانت الممارسات المرتبطة بها من محركات البحث تتغير في الواقع. ولا يزال من الصعب تقييم الكثير من المعلومات حول سياسات الخصوصية التي تقدمها محركات البحث ومن الصعب التحقق من صحتها.

وعلى الرغم من ذلك، تعتبر محركات البحث هي الشركات التي تواجه المستهلك، والتي تعتمد على ثقة المستخدم والعميل في تنفيذ مهامها. وقد ينتج عن فقدان الثقة عواقب فورية مباشرة على قدرة محركات البحث في البقاء ومواصلة أعمالها المربحة. فبقدر ما يكون الأمل في نضوج سوق البحث، تكون المنافسة المتزايدة بين محركات البحث لإثبات التزامها بخصوصية المستخدم. وهذا لا يعني عدم وجود آثار «الارتباط الشديد» وقد يعتمد المستخدمون بشكل متزايد على محركات البحث. ومن المحتمل لبعض خواص محركات البحث مثل السرعة والربط بالشبكات الاجتماعية أو حسابات البريد الإلكتروني أن تعتبر جزءاً من تجربة البحث من قبل المستهلكين ومن ثم يتوقع تقديمها من جانب المزودين الآخرين بمحركات البحث، مما يرفع من مستوى الصعوبة أمام المقبلين على الانخراط في سوق محركات البحث. وفي نفس الوقت تعتمد آثار «الارتباط الشديد» اعتماداً كبيراً على ممارسات البحث المعتادة، والتي يمكن أن تتغير بسرعة نسبية إذا تبين وجود خرق شديد للثقة.[71] إن الثقة في محركات البحث بطرق عدة تعطي فهماً أكبر فيما إذا كان محتوى الإنترنت مهم وجدير بالثقة من عدمه.[72] ومع نمو الإلمام بوسائط الاتصال ببطء بين عامة الناس، قد يحدونا الأمل في أن يخفف الاعتماد على محركات البحث من أثر «الارتباط الشديد» الحالي، وبالتالي تزداد المنافسة على مسائل رئيسية أخرى مثل الخصوصية.

3.2.2. شبكات التواصل الاجتماعي

على الرغم من أهمية آثار «الارتباط الشديد» المشار إليها لبعض محركات البحث وخدمات معينة مرتبطة بها، فقد تكون هذه الآثار ذات أهمية أكبر في شبكات التواصل الاجتماعي (أنظر المربع أدناه لمزيد من التفاصيل). إذا كان صحيحاً أن شبكة «الفيسبوك (Facebook) حققت نجاحاً كبيراً في أن تصبح موقعاً لا غنى عنه

---

70 كوبر، إيه (.Cooper, A) (2007). المنافسة على الخصوصية. مركز الديمقراطية والتكنولوجيا. تم الاسترجاع في 12 ديسمبر/ كانون الأول

71 سي آند باندويل، إل (.See and Banwell, L)، راي كي. (.Ray, K)، كولسون جي. (.Coulson, G)، أوركاهارت سي (.Urquhart, C)، لونسدال آر (.Lonsdale, R)، أرمسترونج سي (.Armstrong, C)، توماس آر (.Thomas, R) وآخرون (2004). إطار رصد وتقييم سلوك المستخدم لدى اللجنة المشتركة لأنظمة المعلومات (JISC). Journal of Documentation، 60(3)، 302–320 و جريفيتيث، جي. (.Griffiths, J) (لا يوجد تاريخ). سلوك بحث الطلاب وشبكة الإنترنت: استخدام المصادر الأكاديمية وجوجل. Library trends، 2005، مجلد 53، رقم: 4، صفحة 539–554، مطبعة The Johns Hopkins University Press.

72 أنظر شاكر ل. (3) (.Shaker, L) إبريل 2006). في جوجل نودع ثقتنا: سلامة المعلومات في العصر الرقمي. First Monday. غوش، ريشاب أيير (Ghosh, Rishab Aiyer)، تم الاسترجاع من http://frodo.lib.uic.edu/ojsjournals/index.php/fm/article/view/1320/1240 وهارجيتاتي، إيه. (.Hargittai, E) (2010). الثقة على الإنترنت: تقييم الشباب لمحتوى شبكة الإنترنت. International Journal of Communication، 4.

بالنسبة للعديد من مستخدميه،»[73] فإن هذا ينتج عنه هذا آثار كبيرة على الخصوصية على الإنترنت. كما أنه يعرض المستخدمين للتغييرات من جانب واحد يقوم بها موقع الفيسبوك (Facebook) والشبكات الاجتماعية الأخرى على سياسات الخصوصية وممارسات الخصوصية المتبعة لديها. ويتم حفظ البيانات الكافية عن المستخدمين في الشبكة الاجتماعية التي لن يقوموا بمغادرتها على الأرجح حتى وإن لم يوافقوا على سياسات الخصوصية فيها، مما يزيد وبشكل كبير من سيطرة الشبكة الاجتماعية على خصوصية مستخدميها.

يقوم نموذج أعمال الشبكات الاجتماعية، مثله مثل محركات البحث، على الإعلانات، وليس ثمة علاقة مالية مباشرة بين مستخدمي الشبكات الاجتماعية والشبكات الاجتماعية نفسها. ولكن تزيد الشبكات الاجتماعية على محركات البحث في هذه الخطوة وذلك نظراً لأن المحتوى الذي تقدمه هو أيضاً بمساهمة المستخدمين. وبما أن معظم المحتوى المقدم من مستخدمي الشبكات الاجتماعية هو عبارة عن معلومات شخصية وبيانات خاصة، فإنه لا يبدو غريباً أن نقول بأن مستخدمي الشبكة الاجتماعية يتبادلون البيانات الخاصة مقابل خدمة «مجانية». ولكن توجد كذلك العلاقات التعاقدية المالية بين الشبكات الاجتماعية وأصحاب الإعلانات من شركائهم، والذين يتولون تمويل الشبكة. ونتيجة لذلك، يكون للشبكات الاجتماعية حافز تجاري طبيعي في الاستمرار بتحسين عملية تحديد أهداف إعلاناتها من خلال الاستعانة بالبيانات الشخصية لمستخدميها. وفي حين قد يكون هناك أيضاً وسائل أخرى لتحقيق الإيرادات في الشبكات الاجتماعية من خلال نماذج الاشتراك أو نماذج المعاملات، إلا إن المصدر الرئيسي لتدفق إيرادات الشبكات الاجتماعية يظل الإعلانات.[74] وبناء على ذلك تبقى البيانات الشخصية للمستخدمين على الشبكات الاجتماعية هي العملة الرئيسية، تلك الكتلة الحيوية التي لابد منها في تحقيق الأرباح من الشبكات الاجتماعية.[75]

6) قوة الارتباط الشديد

«إن وجود مكان واحد نقوم فيه بكل الاتصالات يجعلنا تحت رحمة سياسات أشخاص يسيطرون على البنية التحتية التي نرتبط بها، والتي تكبحنا باستخدام ما نحن مرتبطون به- فلا يمكننا مغادرة الفيسبوك (Facebook) دون ترك كل من نعرفهم- لأن كل من نعرفهم هم على موقع الفيسبوك (Facebook). لم أكن من مستخدمي الفيسبوك (Facebook)، بل كنت من معارضيه. ورأيت أن من عيوبه أنه يجمع كل اتصالاتنا في مكان واحد، فلم تعجبني آثار الخصوصية، ولم أحب الرقابة عليه لبعض الأشياء مثل صور الأمهات المرضعات [...] ورأيت أن هذه سياسات سيئة وكان رد فعلي عدم الانضمام إليه لسنوات رغم وجود جميع أصدقائي عليه [...] انضممت إلى الفيسبوك (Facebook) في أواخر العام الماضي [...] بسبب وفاة صديق لي. كان اسمه تشاك (Chuck)، كان شخص ذكي وقضى الكثير من حياته على الإنترنت. وكان من بين مستخدمي الفيسبوك (Facebook)، وتشارك مع أصدقائه بعض الأشياء من خلاله- وعندما توفى تذكرت أني لم أتواصل معه منذ وقت بعيد [...] فلم أقابلة في مكان تواجده، لأنني لم أكن على الفيسبوك (Facebook). وشعرت بأنني افتقد

73 يورك جي سي (York, J. C.) (2010). مراقبة محتوى النطاق شبه العام. بوسطن، ماساشوسيتس: Open Net Initiative Bulletin. مركز Berkman Center. جامعة هارفارد.

74 لمناقشة موسعة لأنماط تمويل الشبكات الاجتماعية أنظر: Enders, A., Hungenberg, H., Denker, H.-P., & Mauch, S. (2008). السلسلة الطويلة للشبكات الاجتماعية. نماذج الإيرادات من مواقع التواصل الاجتماعي. مجلة European Management Journal, 26(3).

75 Mueller, P. (2011). Offene Staatskunst – Strategie für eine vernetzte Welt. Arbeitskreis Internet Governance. Munich, Germany: Münchner Centrum für Governance-Forschung (MCG)

إلى شيء كبير. وهذا ثمن عدم انضمامي إلى الفيسبوك (Facebook) – لذلك انضممت إليه لأنني قررت بقوة معتقداتي أن أتواجد مع أصدقائي وأتحدث لهم – هذه هي قوة الارتباط الشديد».[76]

دائماً ما يقال بأن مستخدمي الشبكات الاجتماعية يوافقون صراحة على هذه الاستخدامات للبيانات الشخصية في شروط الخدمة وسياسة الخصوصية. وهذا القول قد يحمي الشبكات الاجتماعية من المسؤولية القانونية، فالموافقة «ذات المغزى» أو «الموضوعية» تفترض أن المستخدمين كانوا (1) على علم بسياسة الخصوصية، (2) قادرين على فهم اللغة القانونية المعقدة المستخدمة في هذه السياسات، (3) على استعداد لبذل الوقت في قراءة هذه السياسات، (4) وقادرين على قبول أجزاء معينة من سياسة الخصوصية دون الأجزاء الأخرى. حتى وإن فعل المستخدم ذلك، فإنه يمكن تغيير سياسات الخصوصية في أي وقت، مما يجعل حتى المستخدم الأكثر دراية بالخصوصية عرضة للتغيرات المفاجئة وغير المتوقعة من جانب واحد على سياسة الخصوصية من قبل مزودي الشبكات الاجتماعية.[77] وأوحي بأن هذه الدرجة من التقلب في التعامل مع البيانات الخاصة هي أشبه «بعدم امتلاك المستأجرين لأي حقوق في خصوصية مسكنهم لأنهم يكتشفون أنهم مستأجرين للجدران والأبواب. يمكنكم غلق الأبواب هذا الأسبوع، ولكن عفواً! لقد تغيرت شروط الخدمة».[78]

وهناك كذلك مسائل مرتبطة «بالعمومية» التي تمارس في الشبكات الاجتماعية والتي تمتد إلى ما هو أبعد من الشبكات الاجتماعية الفعلية نفسها. فلقد أصبح من المعتاد لبعض البرامج الآلية أن «تنقب» عن البيانات الشخصية المتاحة بشكل عام على مواقع الشبكات الاجتماعية. ومن ثم لا تحتاج البيانات الشخصية أن تتوفر بشكل عام إلا لفترة قليلة، وبعدها سيتم توزيعها بالفعل على العديد من المواقع الأخرى والفضاء الالكتروني والأنظمة التقنية.[79] في حين إمكانية وجود هذا الخطر بمثل هذه الدرجة في خدمات الإنترنت الأخرى، إلا إن الكم الهائل من البيانات الشخصية المخزنة على مواقع التواصل الاجتماعي تجعل خطر الكشف غير المقصود عن البيانات الخاصة أكبر بكثير من الخدمات الأخرى المماثلة. حيث تتفاقم هذه المشاكل من خلال العمليات اليومية للعديد من مواقع التواصل الاجتماعي التي عادة ما يديرها خبراء ومهندسون في علم الحاسوب. وفي هذا السياق، يتم تطوير المنتجات والخدمات بعد أي منطق هندسي لتزويد العملاء بالمنتجات الجديدة الأكثر تقدماً ووضع سياسة خصوصية في اللحظة الأخيرة. وطوال فترة البحث التي أعد فيها هذا التقرير، ظل هذا البعد التنظيمي الداخلي ضمن الشبكات الاجتماعية في الظهور كحاجز كبير أمام توفير قدر أكبر من الخصوصية للمستخدمين.

4.2.2. الهواتف النقالة والهواتف الذكية والإنترنت عبر الهاتف النقال

لقد ساهمت ثورة استخدام الإنترنت عبر الهاتف النقال في القرن الواحد والعشرين في كثير من المخاوف القائمة حول حماية الخصوصية والبيانات على شبكات الهاتف النقال. فبالمقارنة مع الاتصالات الثابتة، فإن اتصالات الهاتف النقال لديها العديد من السمات التي لها تأثير سلبي جداً على الخصوصية. تشمل

---

76 فاسيل جي.(2011) .Vasile, J. تقديم صندوق الحرية. Elevate 2011 – الموسيقى والفنون والحوار السياسي. جراز، النمسا: Verein zur Förderung des gesellschaftspolitischen und kulturellen Austausches

77 مركز معلومات الخصوصية الالكترونية. (2011). خصوصية شبكات التواصل الاجتماعي. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من /https://epic.org/privacy/socialnet

78 توفيكسي زي، (2010) (.Tufekci, Z). الفيسبوك: خصخصة خصوصياتنا وحياتنا في المدينة المملوكة للشركة. علم الاجتماع التقني: أدواتنا وحياتنا. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011 من http://technosociology.org/?p=131

79 للتعرف على نظرة عامة عن المشكلات والحلول، انظر (2009) .Fuchs, C. مواقع التواصل الاجتماعي ومجتمع المراقبة، دراسة حالة حرجة لاستخدام studiVZ وFacebook وMySpace من جانب الطلاب في سالزبورغ في سياق المراقبة الالكترونية. سالزبورغ: نظرية المعلومات الموحدة لــ Forschungsgruppe.

هذه الأجهزة أدوات تعريف هوية الهاتف النقال (IMEI) وبطاقة IMSI) SIM)، والقدرة على التأكد بانتظام من الموقع الجغرافي من الجهاز النقال، وقدرة الآخرين على اعتراض الاتصالات اللاسلكية المتنقلة لانتقالها عبر الهواء.[80] ويتعين دراسة هذه المخاوف، وخاصة تلك المتعلقة بالإنترنت عبر الهاتف، بالإضافة إلى المخاوف القائمة بشأن الخصوصية على الإنترنت، والتي تنطبق جميعها أيضاً على أجهزة الإنترنت النقالة.

في حين يفترض في كثير من الأحيان أن هذه المخاوف لا تتصل إلا «بالهواتف الذكية»، فهي تنطبق بقدر مساو على أي جهاز نقال قادر على الوصول إلى الإنترنت من خلال شبكات الهاتف المحمول. وبالتالي يتعين تناول هذه المخاوف المتعلقة بالخصوصية في البلدان النامية والبلدان المتقدمة بشأن أي جهاز قادر على الوصول إلى الإنترنت. فهي تنطبق على المزارع الموجود في زيمبابوي الذي يقوم بإرسال رسائل إلكترونية إلى أسرته على هاتف نوكيا القديم، بنفس القدر عند إرسال محام الشركات في هونغ كونغ باستخدام جهاز أي فون (iPhone) رسالة إلكترونية إلى الموكل. وعلى الرغم من وجود المخاوف فيما يتعلق بالهواتف النقالة بشكل عام، فهي تتفاقم أكثر عند استخدام الإنترنت على الأجهزة الهاتف النقال.

ومع ذلك، فضلاً عن المخاوف المحددة المتعلقة بالخصوصية على شبكات الهاتف النقال نفسها، تثير الهواتف الذكية أيضاً مخاوف إضافية تتعلق بالخصوصية بالمقارنة مع الهواتف «الأقل ذكاء»، والتي غالباً ما يطلق عليها اسم "الهواتف المميزة». عادة ما تستخدم الهواتف الذكية كأجهزة إنترنت نقالة وعادة ما تكون قادرة على نقل بيانات أكثر بكثير من الهواتف النقالة العادية من خلال ما يسمى بشبكات الجيل الثاني (2G) أو الثالث (3G) أو الرابع (4G) للهاتف النقال، وهذا يعني أيضاً أنها قادرة على نقل بيانات شخصية أكثر بكثير من الهواتف النقالة العادية من خلال شبكة الإنترنت العامة. وعلاوة على ذلك، فقد تم تصميم هذه الهواتف لتكون "دائماً» متصلة بالإنترنت. فضلاً عن ذلك، يتم تركيب مجموعة متنوعة من الخدمات ضمن أجهزة الهواتف الذكية لترسل بيانات عبر شبكة الإنترنت بشكل منتظم، وغالباً دون معرفة المستخدم للهاتف. فقد تم توثيق أن الهواتف الذكية التي تعمل بنظام Google Android وApple iPhone تقوم بشكل منتظم "بالاتصال بمصدرها" وبالتالي تنقل معلومات حول موقعها وحول المستخدم وغير ذلك من المعلومات الشخصية مثل شبكات Wi-Fi في نطاق الإنترنت.[81]

ويساهم هذا في الاتجاه العام في خصوصية الهاتف الذكي، أي تجزئة السيطرة على البيانات الشخصية في منصات الإنترنت عبر الهاتف النقال، بحيث يكون لكل من مزود خدمة الإنترنت عبر الهاتف النقال، والشركة المصنعة للجهاز، ومزود نظام التشغيل، ومزود التطبيقات جميعاً قدر معين من السيطرة على البيانات الشخصية للمستخدم. فعندما يقوم أحد مستخدمي الهاتف الذكي بإرسال رسالة بريد إلكترونية من الأرجنتين، فإنه قد يتم السيطرة على بعض بياناته الشخصية من قبل الشركة المصنعة للجهاز (Samsung)، ومزود نظام التشغيل للهاتف (Google)، ومزود خدمة الإنترنت المتنقل (Movistar)، ومزود تطبيقات البريد الإلكتروني (K-9 Mail)، ومزود خدمة البريد الإلكتروني (Yahoo) ومقدم خدمة البريد الإلكتروني للشخص المرسل إليه (Microsoft). مع العلم بأن هذا الأمر لا يشتمل على مسائل تسرب البيانات عند إرسال كلمات المرور ومحتوى البريد الإلكتروني دون تشفير عبر الإنترنت، أو احتمالية الاطلاع على مزيد من البيانات الشخصية من قبل أجهزة تنفيذ القوانين المحلية أو الدولية أو إطلاع أطراف ثالثة غير مصرح لها على تلك البيانات الشخصية، ولا تأخذ في الاعتبار طبقة التعقيد الإضافية التي تنتج عن تثبيت تطبيقات إضافية على الهواتف الذكية («Apps")، والتي قد يكون لها هي الأخرى قدرة للحصول على البيانات الشخصية للمستخدمين. يضاف إلى ذلك أن الهواتف الذكية تجمع بين باقة واسعة من أجهزة الاستشعار ورقائق

---

80 مؤسسة Electronic Frontier Foundation. أجهزة الهاتف النقال. مشروع الحماية الذاتية من المراقبة. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من https://ssd.eff.org/tech/mobile.

81 Angwin, J., & Valentino-Devries, J. (2011) أجهزة الهاتف النقالة Apple's iPhones و Google's Androids ترسل موقع الهاتف الخلوي. مجلة Wall Street Journal. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html

ومنصات الاتصالات المختلفة، مما يصعب على مستخدميها فهم الآثار المترتبة على خصوصية كل جهاز من أجهزة الاستشعار الإضافية أو لرقاقة محددة من رقاقات الاتصالات. ويشمل الهاتف الذكي الصادر مؤخراً iPhone4S رقائق اتصالات قادرة على التواصل عبر أنواع مختلفة من شبكات الهاتف النقال (/GSM/CDMA EDGE/ UMTS/HSDPA/HSUPA)، وشبكات الإنترنت اللاسلكية Wi-Fi (802.11b/g/n)، وأنظمة تحديد المواقع العالمية (GPS) وتقنية (Bluetooth)، فضلاً عن أجهزة استشعار الضوء والقرب والحركة والمعروفة باسم جيروسكوب (gyroscope) وميكروفونات متعددة.[82]

7) استغلال تخزين أجهزة الإنترنت

في الكثير من الدول القمعية حول العالم، من المعتاد إجبار السجناء السياسيين الذين تم القبض عليهم على تسليم أجهزتهم المتصلة بالإنترنت قبل استجوابهم. والشيء الأكثر أهمية للسلطات هي الهواتف الذكية لأنها تحمل قدرا هائلاً من البيانات الخاصة الإضافية التي لا تتوفر عادة على الهواتف النقالة العادية. ثم يتم استخدام هذه المعلومات الشخصية لجمع المعلومات الشخصية بصورة منهجية من على شبكات التواصل الاجتماعي التي يستخدمها السجناء السياسيون. وبهذه المعلومات يمكن استهداف الاتصالات الأخرى المباشرة وغير المباشرة للسجناء السياسيين. وتشتمل هذه الشبكات على شبكات شخصية ومهنية وأخرى طارئة لأفراد يخافون أو يسجنون دون سبب إلا لكونهم تقابلوا بالشخص الخطأ – ولو لفترة وجيزة. هذه الأساليب لا تساعد بالضرورة في أي غرض مشروع حكومي، بل هي تعمل على تخويف الأفراد وشبكاتهم الشخصية. ويمكن تصميمها من أجل التأثيرات المروعة ونشر شبح السيطرة الحكومية أبعد من السجناء السياسيين أنفسهم. وتعتبر أجهزة الاتصالات الشخصية والبيانات الشخصية التي يقومون برقمنتها (تحويلها إلى رقمية) وجمعها هي من العناصر الأساسية في استراتيجيات التخويف هذه.

ويمكن الجمع بين أجهزة الاستشعار هذه بطرق غير متوقعة، مثل المحاولات الأخيرة لإنشاء سجل من طباعة المستخدم باستخدام جهاز استشعار الحركة Gyroscope.[83] ويتم تخزين الكثير من البيانات التي تم جمعها من خلال الهواتف الذكية على الهاتف لفترة غير محددة من الزمن، ولا يستطيع المستخدم التحكم في إبقائها أو مسحها إلا في نطاق قليل جداً. وبناء على مدى استخدام الهواتف الذكية، يمكن أن تصبح تلك الهواتف وبسرعة عبارة عن مستودعات رقمية تضمن كل تفاصيل حياة أصحابها. وهذا يعني أنه في حال فقدان الهواتف الذكية أو سرقتها أو مجرد أخذها من أصحابها، فإن الآثار المترتبة على خصوصيتهم قد تكون شديدة (أنظر المربع لمزيد من التفاصيل).

وأخيراً، تستخدم كذلك شركات أنظمة الهواتف الذكية المهيمنة، مثل Google Android وApple iPhone أنظمتها في استهداف المستخدمين بإعلاناتها. فالبيانات التي حصلت عليها هذه الشركات عن المستخدمين من أجهزة الإنترنت الأخرى – من خلال تاريخ البحث على جوجل أو تاريخ الشراء على ITunes Store أو تاريخ استخدام حساب جوجل/ابل، أو ما شابه ذلك – يمكن دمجها في كثير من الأحيان مع البيانات المقدمة من نظام الهاتف المتنقل مثل بيانات الموقع الجغرافي من الهاتف. هذه المعلومات الشخصية عن الفرد – التي قد تكون في كثير من الأحيان أكثر شمولية مما يعرفه المستخدم نفسه – تسمح لهذه الأنظمة الأساسية

---

82 Higginbotham, S. (2010). أجهزة استشعارiPhone 4 تسلط الضوء على VCs. GigaOM. تم الاسترجاع من: http://gigaom.com/2010/06/08/iphone-4-sensors-highlight-a-bright-spot-for-vcs/

83 كاي إل و تشين إتش (Cai, L., & Chen, H.) (2011). TouchLogger: استنتاج ضغطات المفتاح على شاشة اللمس من حركة الهاتف الذكي. فعاليات HotSec'11 خلال مؤتمر USENIX السادس حول المسائل الشائكة في الأمن. بيركلي، كاليفورنيا، الولايات المتحدة الأمريكية: USENIX Association

باستهداف المستخدمين بإعلاناتهم المخصصة. وكما هو الحال بالنسبة لمحركات البحث وشبكات التواصل الاجتماعي، فإن لمطوري الأنظمة الأساسية المستخدمة في الهواتف النقالة مصلحة تجارية في الحصول على أكبر قدر ممكن من المعلومات الشخصية من مستخدميها. فكلما زادت المعلومات التي يعرفونها عن مستخدميهم، كلما زادت قيمة الإعلانات المستهدفة التي تظهر على أنظمة الإنترنت في الهواتف الذكية.

5.2.2. محددات هوية فريدة للمواطنين ومبادرات الحكومة الإلكترونية

قبل ظهور الإنترنت العام بفترة طويلة في أوائل التسعينيات، اتجهت الحكومات في جميع أنحاء العالم نحو توحيد السجلات المتعلقة بمواطنيها وجمعها في سجل مركزي. ومع ازدياد القدرة الحاسوبية وانخفاض تكلفتها، أصبح في استطاعة الدول تحقيق مكاسب كبيرة فيما يتعلق بالكفاءة داخل أنظمتها عن طريق مركزة وتوحيد المعلومات المتعلقة بالمواطنين.[84] وفقاً لآراء جيمس سي. سكوت (James C. Scott)، سعت الدول إلى جعل المجتمعات الخاضعة لحكمها مجتمعات «واضحة» كي تعزز من سياساتها.[85] كما أنها عملت على الاستجابة للمطالب المستمرة على البيروقراطيات العامة لخفض التكاليف بزيادة الكفاءة من خلال استخدام الحوسبة. وقد كان لهذه المكاسب التي حققت في الكفاءة تأثيرات سلبية على خصوصية المواطنين وسرية هويتهم. وقد واجه مناصرو الخصوصية المبادرات العامة لإنشاء قواعد بيانات كبيرة عن المواطنين بالتشكيك، حيث تجلت مخاطر قواعد البيانات هذه عند فقدان المعلومات (أنظر الشكل أدناه لمزيد من التفاصيل).

تشتمل قواعد البيانات هذه وخدمات تحديد الهوية على عنصر متصل بالإنترنت، وهو ما يسمح للمواطنين بالوصول إلى الخدمات الحكومية المختلفة عبر شبكة الإنترنت. وقد يحصل المواطنين على الكثير من الفوائد عند استخدام هذه الخدمات، مثل زيادة مستوى السرعة والكفاءة. ولكن كما أشار إليه فريق العمل المعني بالخصوصية لدى الحكومة الأمريكية:

«هذه الفوائد على الرغم من ذلك لا تأتي دون مقابل: بل الثمن هو فقدان الخصوصية. والخصوصية في هذا السياق تعني «خصوصية المعلومات»، مطالبة الفرد للسيطرة على الشروط التي يتم بموجبها اكتساب المعلومات والكشف عنها واستخدامها – أي المعلومات التي تحدد هوية الفرد.[86]

8) فقدان البيانات الشخصية لـ 25 مليون مواطن

وقعت واحدة من أكبر خسائر بيانات المواطنين في أوروبا في المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية عندما فقدت اثنين من الأقراص المدمجة (CD) التي تحتوي على البيانات الشخصية لأكثر من 25 مليون شخص في النظام البريدي الداخلي للحكومة في العام 2007.[87] حيث تم إرسالها دون أي آليات حماية تقنية من إدارة الإيرادات والجمارك البريطانية (HMRC) إلى مكتب التدقيق الوطني (NAO)، فضلاً عن تدني مستوى الرقابة الحكومية الفعلية على نقل الأقراص المدمجة، وذلك لنقل

---

84 للاطلاع على مناقشة بشأن أهمية الحوسبة للدولة والمجتمعات الحديثة أنظر (1998) .Robertson, D.S النهضة الجديدة: أجهزة الحاسوب والمستوى التالي من الحضارة. مطبعة جامعة أكسفورد. الولايات المتحدة الأمريكية.

85 سكوت جي سي (1998) (.Scott, J.C) المراقبة مثل الدولة: كيف أخفقت بعض البرامج للتحسين من الوضع البشري. نيو هافين: مطبعة جامعة ييل.

86 جيتس جي (.Gates, J) وفريق العمل المعني بالخصوصية (1995). الخصوصية والبنية التحتية القومية: مبادئ تقديم واستخدام المعلومات الشخصية. لجنة سياسة المعلومات، فريق عمل بنية المعلومات التحتية. تم الاسترجاع من http://aspe.hhs.gov/datacncl/niiprivp.htm

87 جورج إم (.Gorge, M) (2008). حماية البيانات: لماذا لم تزل المؤسسات غير مدركة للمسألة الأساسية؟ الاختيار الحاسوبي والأمن، 8–5 ،(6) 2008.

هذه الأقراص المدمجة بواسطة خدمة البريد السريع الخاص. كانت المعلومات الشخصية التي احتوت عليها هذه الأقراص تتعلق بمبالغ إعانات الأطفال لجميع الأسر في المملكة المتحدة. وبما أن هذه الإعانة تشمل الغالبية العظمى من الأسر في المملكة المتحدة، فقد أثر فقدان البيانات الشخصية تقريباً على جميع الأسر التي لديها أطفال دون سن 16 سنة. وقد قيل بأن الغالبية العظمي من البيانات الشخصية التي تعرضت للخسارة واسعة النطاق هي تتعلق بالقطاع العام.[88] ويعزى هذا عادة إلى الإخفاق «في تعزيز ثقافة الأمن للبيانات الشخصية"،[89] سواء كانت متصلة أو غير متصلة بالإنترنت.

يصف هذا البيان الثاقب صعوبة ضمان فعالية الحكومة الإلكترونية وكذلك ضمان الخصوصية، بل يمكن أن يوجد هذا التوتر أيضاً في أشكال أحدث من الحكومة الإلكترونية. فعادة ما تهدف هذه المبادرات إلى زيادة مشاركة المواطنين والشفافية في العمليات الحكومية، ولكن تصطحبها مخاوف تتعلق بالخصوصية. فمن ناحية، يكون على المستخدمين المشاركين في هذه المبادرات تعريف أنفسهم كمواطنين في المبادرات الحكومية المتاحة للمشاركة، لأنه من غير الممكن مشاركة غير المواطنين. ثم يتوقع منهم المشاركة في هذه المبادرات "بهويتهم الكاملة". ولا يسمح بالمشاركة "دون ذكر الهوية أو المشاركة باسم مستعار" - حتى بالنسبة للأفراد المحددين على أنهم من المواطنين.

من النقاط الأخرى ذات الأهمية ذلك التوتر القائم بين الشفافية ومبادرات الحكومة المتاحة (openGovernment) أو بين المبادرات الحكومية المتاحة للمشاركة والخصوصية. حيث إن معظم المبادرات الحكومية المتاحة للمشاركة تتطلب مستويات عالية من الشفافية لضمان نزاهة العمليات. وهي بذلك تخاطر بتقييد حق الأفراد في الوصول إلى بياناتهم الشخصية من أجل حماية الشفافية. ويمكن للحكومة المستخدمة للنظام أن تحل مشاكل التحقق من الهوية من خلال توقيع المواطنين على عرائض أو المشاركة في الحكومة المتاحة (openGovernment) باستخدام الاسم الحقيقي، ولكن يؤدي ذلك إلى تقييد حرية التعبير لدى المستخدمين مقارنة بوضعهم إذا كانوا مجهولين أو يتحدثون بأسماء مستعارة من خلال طرف ثالث موثوق به.

وأخيراً، من المهم أن ننظر في التعاون الوثيق مع القطاع الخاص في الكثير من مبادرات الحكومة الإلكترونية (eGovernment) والحكومة المتاحة (openGovernment). فمع افتقار الحكومات في كثير من الأحيان للقدرة على أداء هذه المهام بنفسها، فإنها تستعين في تنفيذ هذه العمليات والخدمات التي هي جزء أساسي من الحكومات الحديثة بمزودي الخدمات من القطاع الخاص. ورغم أن هذا قد يمثل وسيلة فعالة للحد من التكاليف، إلا أنه يعرض مخاطر إضافية بشأن الخصوصية وذلك عند إدخال أطراف ثالثة في نقل ومعالجة وتخزين البيانات الشخصية للمواطنين. وهذه التفاعلات مع القطاع الخاص لا تضر بالضرورة بخصوصية المواطنين، بل هي توفر طبقة إضافية من التعقيد الذي لابد من إدارته بشكل مناسب.

88 المنظمة الدولية لحماية الخصوصية (2011) .(Privacy International). المملكة المتحدة – نبذة عن الخصوصية. المنظمة الدولية لحماية الخصوصية (Privacy International).
تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من https://www.privacyinternational.org/article/united-kingdom-privacy-profile

89 المرجع السابق.

2.3. التهديدات التي تشكلها الآليات المختلفة في المراقبة وجمع البيانات

1.3.2. تحديد هوية المستخدم – معرفات الهوية الفريدة، ملفات تعريف الارتباط (seikooC) وأشكال أخرى من أشكال تعريف هوية المستخدم

ثمة كم هائل من الوسائل المختلفة التي يتم من خلالها تحديد هوية مستخدمي الإنترنت، بدءاً من التسجيل الأولي لمستخدمي الإنترنت من خلال مزودي خدمات الإنترنت أو في مقاهي الإنترنت، إلى ترقيم وتحديد أجهزة الإنترنت التي غالباً ما تكون مرتبطة بحسابات على الإنترنت، إلى معرفات الهوية الفردية التي توفرها متصفحات الإنترنت أو تحفظها ملفات تعريف الارتباط (Cookies)، فضلاً عن عناوين بروتوكول الإنترنت (IP) التي يتم تخصيصها لمستخدمي الإنترنت من خلال بروتوكولات الإنترنت. جميع هذه الإجراءات قد تساعد في إظهار هوية مستخدم الإنترنت، ولكن في بعض الحالات قد تكون هذه الهويات أيضاً ضرورية لتقديم الخدمات على شبكة الإنترنت. ومن الصعب استخدام الإنترنت دون وجود عنوان بروتوكول إنترنت (IP) على الرغم من إمكانية تخصيصه بشكل ديناميكي أو دون إظهار هويته – وتعتمد العديد من خدمات الإنترنت الأخرى كل منها على شكل من أشكال تحديد الهوية.

إن من مخاوف الخصوصية في العالم النامي على وجه التحديد، وفي بعض أجزاء من العالم المتقدم، تسجيل المستخدم على الإنترنت، سواء للاستخدام قصير الأمد أو طويل الأمد. فقد يتم تعريف هوية المستخدم كجزء من إجراءات التسجيل في مقهى الإنترنت أو كجزء من إجراءات الاشتراك في الشبكة اللاسلكية أو من خلال شراء هاتف نقال. وفي كل من هذه السياقات تساهم آليات تعريف هوية المستخدم على الإنترنت في وضع قيود على الخصوصية وسرية الهوية على الإنترنت. ومن أسباب المخاوف الأخرى تقييد التعبير دون الكشف عن الهوية والتأثيرات المروعة التي تنتج عن آليات تعريف الهوية هذه. فمن المؤكد أن إجراءات تعريف الهوية هذه تتميز بالشفافية النسبية على الأقل لمستخدمي الإنترنت، وهي ما لا يوجد في غيرها من آليات تعريف هوية المستخدم.

لعل من أشهر آليات تعريف هوية المستخدم الأقل شفافية ملفات تعريف الارتباط (Cookies)، والتي يتم تخزينها على جهاز حاسوب مستخدم الإنترنت عند زيارته لموقع من المواقع على شبكة الإنترنت، واستخدام متصفح الإنترنت. وبناءً على طريقة إنشاء هذا الموقع وضبط أوضاع متصفح المستخدم، يمكن تخزين أو تحديث من واحد إلى عشرات ملفات تعريف الارتباط (Cookies) عند زيارة موقع من المواقع؛ ومن خلال تخزين ملفات تعريف الارتباط (Cookies) على أجهزة المستخدمين، يمكن تتبع كل مستخدم على الإنترنت. وبالنسبة لملفات تعريف الارتباط (Cookies) التي يتم ضبطها خارج النطاق الذي يزوره المستخدم – وتسمى بملفات تعريف ارتباط الطرف الثالث – يمكن لها أن "تتبع" المستخدمين في معظم أجزاء شبكة الإنترنت.

وتشكل ملفات تعريف الارتباط كذلك عنصراً من عناصر تحليلات المستخدم، وهي من الطرق الشائعة لتتبع المستخدم عبر شبكة الإنترنت. وتوحي التقديرات الموثوق بها أن ما بين 40 و 60% من أكبر مواقع الإنترنت تستخدم برنامج Google Analytics، وهي أداة تتبع حركة التصفح وتسمح للمسؤولين بقياس حركة المرور.[90] وتوحي تقديرات مشابهة بأن ما يقدر بـ 70% من جميع مواقع الإنترنت تستخدم نوعاً من أنواع تتبع المستخدم استناداً إلى حزم تحليلات مختلفة للإنترنت.[91]

---

90 (2011) BuiltWith. إحصاءات استخدام Google Analytics – مواقع الإنترنت المستخدمة لبرنامج Google Analytics. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من http://trends.builtwith.com/analytics/Google-Analytics

91 (2011) W3Techs. إحصاءات الاستخدام وحصة السوق من أدوات تحليل حركة المرور في المواقع الالكترونية. خدمات Q-Success على الإنترنت. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من http://w3techs.com/technologies/overview/traffic_analysis/all.

لقد تطورت التطبيقات التقنية لملفات تعريف الارتباط لفترة طويلة وتجاوزت نقطة تحكم المستخدمين في عدم تتبعهم. فهذه الملفات غالباً ما تتواجد لسنوات على جهاز الكمبيوتر الخاص بالمستخدم ويتم تمديدها تلقائياً في كل مرة يقوم المستخدم بزيارة موقع على الشبكة المرتبطة بها. ويمكن أيضاً وضعها من خلال الوظائف الإضافية (add-ons) للمتصفح مثل "Adobe Flash" بشكل مستقل عن المتصفح الرئيسي. وإذا حاول المستخدم إزالة هذه الملفات من أي مكان من الأماكن العديدة التي يمكن أن تخزن فيها، فإنها تعود مرة ثانية من مناطق تخزين أخرى أو باستخدام آليات تعريف أخرى مثل معرفات جلسات العمل (Session Ids)، والوظائف الإضافية (Add-ons) للمتصفح وبرامج التخزين المؤقت لملفات التعريف أو أي من الوسائل الأخرى التي تسمح بإعادة إنشائها دون موافقة المستخدمين الفرديين.[92] ورغم كثرة الجدال عن مخاوف الخصوصية المرتبطة بملفات تعريف الارتباط في بداية تطور شبكة الإنترنت العامة، فلا تزال العديد من المسائل المرتبطة بذلك عالقة دون حل.[93]

وعلى الرغم من ذلك، نجد أن ملفات تعريف الارتباط ما هي إلا مكون من العديد من المكونات المستخدمة في تعريف هوية المستخدم على شبكة الإنترنت. وهي تعمل من خلال النموذج الممول عن طريق الإعلانات والتي تتخلل الكثير من مواقع الإنترنت وتستفيد من تعريف هوية المستخدمين لغرض استهدافهم بالإعلانات. وفي حين يتاح للمستخدم كثيراً فرصة تخصيص أوضاع الموقع الالكتروني والإعلانات الأكثر صلة وذلك على شكل حوافز للمستخدمين لقبول أو حتى دعم تتبع الإنترنت، فمجرد تعقب المستخدمين عبر الإنترنت يمثل دافع ربح واضح. ومن الأمثلة الأخرى على مصالح الأعمال ردود الفعل العنيفة من جانب صناعة إعلانات الإنترنت على تشريع حظر التعقب (DoNotTrack) الأخير في أجزاء مختلفة من العالم.[94] وعلى الرغم من اعتماد جزء كبير من صناعة الإنترنت على عائدات الإعلانات في التمويل، إلا إن إيجاد سبل تجنب تعريف هوية الخصوصية والتعقب المخترق للخصوصية على الإنترنت يبقى أمراً في غاية الصعوبة.[95]

2.3.2. برامج الدعاية (erawdA) والبرمجيات المؤذية (erawlaM) وبرامج التجسس (erawypS) التي تسمح بالدخول والمراقبة بالبيانات الخفية

تنشأ تهديدات أخرى أمام خصوصية المستخدمين على شبكة الإنترنت نتيجة لبرامج الدعاية (adware) والبرمجيات المؤذية (malware) والفيروسات، حيث تقوم هذه البرامج في بعض الحالات بجمع المعلومات الشخصية للمستخدم واستخدامها في أغراض إجرامية، مثل سرقة المال من الأفراد واختراق حسابات الإنترنت الخاصة بهم أو إساءة استخدام معلوماتهم الشخصية بأي طريقة أخرى. وتستخدم كذلك برامج التجسس بشكل شائع من قبل المستخدم الراغب في مراقبة المستخدمين الآخرين الذين يعرفهم معرفة شخصية. وكثيراً ما تستخدم برامج التجسس هذه من جانب الملاحقين الذين يرغبون في التعدي على الحياة الشخصية لضحاياهم. وقد تتضمن نقل تفاصيل المكان الفعلي للفرد واتصالاته ومعلومات شخصية أخرى وكلمات

---

92 ماير جي (2011). تتبع المتتبعين: إعلانات مايكروسوفت. مركز الإنترنت والمجتمع، كلية حقوق ستانفورد. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من http://cyberlaw.stanford.edu/node/6715

93 لمزيد من المعلومات انظر RFC 2109: https://www.ietf.org/rfc/rfc2109.txt

94 كلارك جي (2011). قوانين حظر التعقب في مواجهة الزخم الأمريكي. The Register. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من http://www.theregister.co.uk/2011/05/06/senate_do_not_track/

95 روني، بي (2011). المملكة المتحدة تنشر المبادئ التوجيهية «لملفات تعريف الارتباط» الصادرة عن الاتحاد الأوروبي. Wall Street Journal. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من http://blogs.wsj.com/tech-europe/2011/05/09/u-k-publishes-e-u-cookie-directive-guidelines/

المرور.[96] والأمر المدهش ربما هو أنه من القانوني تماماً شراء وبيع هذه التقنيات في أجزاء كثيرة من العالم. ولذلك فإن من السهل نسبياً للأفراد الذين يرغبون في إساءة استخدام هذه التقنيات الوصول إليها.

تندرج برامج الدعاية (adware) ضمن فئة البرمجيات المعتدية على الخصوصية والمتجاهلة لموافقة المستخدم، وهي برمجيات يتم تخزينها على أجهزة الكمبيوتر دون قصد. وهي عبارة عن برمجيات يصعب على المستخدمين إدراكها لأنها عادة ما تظهر في شكل برنامج مكافحة الفيروسات أو أداة بحث أو تقنية ‹مفيدة› مماثلة يرغب المستخدم في استخدامها. كما أنها وغالباً ما تتجمع مع البرامج التي تبدو مجانية. ولكنها تستخدم لإظهار إعلانات غير مرغوب فيها للمستخدم وتتبع سلوكه على جهاز الكمبيوتر.

ومن الجدير بالذكر أيضاً قيام أجهزة تنفيذ القانون باستخدام تقنية حصان طروادة (Trojan Horse) لجمع المعلومات من أجهزة الكمبيوتر البعيدة. ولقد كانت هذه الممارسات محل جدل كبير في أجزاء كثيرة من العالم لاشتمالها على السيطرة الكاملة في كثير من الأحيان على جهاز الكمبيوتر. وتستخدم هذه التقنية كشكل من أشكال ما يسمى بـ«الاعتراض القانوني»، رغم أن المجتمع المدني يعتبر هذه التقنية من البرمجيات المؤذية (malware) ويعتبرها مزودو برنامج مكافحة الفيروسات على أنها فيروسات.[97] هذه الاستخدامات لا تترك مساحة كبيرة للبيانات الشخصية الخاصة، والتي يتم تخزينها على أجهزة الكمبيوتر، على الرغم من أن هذه المساحة من "الكرامة الشخصية الحساسة العميقة» يتم حمايتها بشكل واضح باعتبارها جزءا أساسياً من كرامة الإنسان في العديد من الولايات القضائية في جميع أنحاء العالم. وأخيراً بدأت البرمجيات المؤذية وبرامج التجسس وبرامج الدعاية تستهدف وبشكل متزايد الأجهزة المتنقلة مثل الهواتف الذكية وأجهزة التابليت (Tablet) وغيرها من الأجهزة الأخرى المتصلة بالإنترنت مثل أجهزة التلفاز الذكية. وهنا يتوقع المستخدمون بأنهم في مأمن وليسوا بحاجة إلى أي حماية إضافية، وبهذا يقعوا فريسة الاستغلال. فمن غير المتوقع دائماً فقدان بياناتك الشخصية من خلال جهاز ليس بجهاز كمبيوتر شخصي (أنظر المربع لمزيد من التفاصيل).

تسمح بروتوكولات الاتصالات المختلفة التي تستخدمها هذه الأجهزة بالعديد من آليات التوزيع المختلفة للبرمجيات المؤذية. حيث يمكن إعادة انتشار فيروس تم تحميله من الإنترنت عن طريق هاتف نقال مرتبط بشبكة اتصال الجيل الثالث (3G) عبر شبكة الإنترنت اللاسلكية (Wi-Fi) أو تقنية Bluetooth إلى أجهزة أخرى في مواقع قريبة جداً. ومع انتشار نظم التشغيل العامة في الأجهزة النقالة مثل نظام تشغيل iOS وAndroid، أصبح من السهل لهذه الأجهزة أن تنشر برمجيات مؤذية بأنظمة تشغيل مماثلة. كما إن وسائل الاتصال المتعددة والإجراءات الأمنية غير الواضحة تجعل من أجهزة الإنترنت الجديدة هدفاً واضحاً للبرمجيات المؤذية وبرامج الدعاية. ومع النمو السريع لعدد الأجهزة المتصلة بالإنترنت، بدءاً من وحدات تحكم الألعاب إلى التلفاز والسيارات والأفران والثلاجات الذكية، أصبح «إنترنت الأشياء (Internet of Things)"»[98] أمراً طبيعياً، حيث وجد المستخدمون أن من الصعب بشكل متزايد إبقاء السيطرة على بياناتهم الشخصية. فالسيارات وأجهزة التلفاز المتصلة بالإنترنت لا توفر في العادة إعدادات الخصوصية أو تسمح للمستخدمين بتثبيت برنامج مكافحة الفيروسات أو جدار حماية. فهذه التطورات تفرض تحديات خطيرة على خصوصية المستخدم وقدرة الفرد على التحكم في بياناته الشخصية.

---

96 مركز معلومات الخصوصية الالكترونية (2011). تقنيات المراقبة الشخصية. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من https://epic.org/privacy/dv/personal_surveillance.html

97 Chaos Computer Club (2011). يقوم Chaos Computer Club بتحليل البرمجيات الخبيثة للحكومة. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من http://ccc.de/en/updates/2011/staatstrojaner.

98 Gershenfeld, N., Krikorian, R., & Cohen, D. (2004). إنترنت الأشياء. Scientific American, 291(4), 76-81. Springer.

9) اختراق شبكة التحكم في الألعاب

في أبريل/ نيسان 2011 تم اختراق شبكة 'Playstation Network' التابعة لشركة سوني (Sony) والمرتبطة بوحدة التحكم في Sony Playstation من قبل مخترقين مجهولين. ونتج عن ذلك وفق الأنباء اختراق البيانات الشخصية الخاصة بـ 77 مليون مستخدم للشبكة، بما في ذلك الاسم والعنوان والبلد وعنوان البريد الإلكتروني وتاريخ الميلاد ورقم بطاقة الائتمان وكذلك اسم الدخول وكلمة السر وإجابات الأمن المستخدمة في كلمة السر بالشبكة.[99] وبصرف النظر عن حجم المعلومات الشخصية المسروقة، استغرق الأمر أكثر من أسبوع لشركة سوني(Sony) حتى تخبر المستخدمين للشبكة أن بياناتهم الشخصية في خطر. ونظراً لشيوع استخدام نفس كلمة المرور عبر مختلف مواقع الإنترنت، فقد عرض هذا الحدث المستخدمين لشبكة Playstation Network للخطر ليس فقط على الشبكة نفسها ولكن على الإنترنت بالكامل.

3.3.2. برامج مراقبة الحزم (IPD)

تعتبر برامج مراقبة الحزم (DPI) من التقنيات المنتشرة والمستخدمة كأداة تحكم عامة في أجزاء كثيرة من الإنترنت. وتتميز هذه التقنية بأنها قادرة على «الاختراق داخل» الحزم التي تنتقل عبر شبكة الإنترنت، ثم تقوم بفحص محتواها وتتفاعل مع هذا المحتوى بطرق مختلفة. إن التقنيات التي تفحص وأحياناً تعدل حركة المرور على الإنترنت تقوم بذلك على أساس معلومات العنوان الخاصة بها. وعلى النقيض من ذلك، تقوم برامج مراقبة الحزم بالبحث 'داخل' الحزمة ومسحها لاستخراج أي كلمات رئيسية أو أنماط أو سمات أخرى معينة ليست واضح من عنوان الحزمة.[100] في حين تجمع هذه التقنية «العديد من مميزات تكنولوجيا الإنترنت التي كانت موجودة لفترة طويلة [...] إلا أن الجمع بين هذه العناصر ووضعها في مجموعة من الممارسات القابلة للتوسيع والمنفذة على نطاق واسع يعتبرها خبراء هذا المجال وخبراء التكنولوجيا ونقاد السياسات على أنها تكنولوجيا جديدة».[101] كما أنها تكنولوجيا ظلت موضوع جدل منذ أن بدأ الحديث عنها. وخلال هذه المناقشات، كانت هذه التكنولوجيا مرتبطة ببعض أكبر التعديات على الخصوصية على شبكة الإنترنت. فعندما سئل أحد مزودي هذه التقنية في حوار أجراه المؤلف عن شعوره عند بيع أجهزة برامج مراقبة الحزم (DPI)، رد قائلاً أنها أشبه بالإصابة بمرض ينتقل عن طريق الاتصال الجنسي.

كان استخدامان من الاستخدامات الأولى لبرامج مراقبة الحزم (DPI) والتي جذبت الاهتمام العام بشكل كبير عبارة عن أهداف دعاية عن طريق Phorm وNebuAd. حيث تم استخدام هذه التقنية في بناء ملفات دعاية واسعة حول المستخدمين من عدة مزودي لخدمات الإنترنت، بل وصل الأمر في بعض الحالات إلى حد إدراج الإعلانات الإضافية في المواقع. ولقد تسبب هذا التلاعب بمواقع المستخدمين وجمع البيانات الخاصة بهم دون موافقتهم في فضيحة لدرجة أن تخلى عنها مزودو خدمات الإنترنت في النهاية وأصبحت جزءا من الإجراءات

---

99 ستوارت كي (2011). اختراق شبكة PlayStation Network: ما يحتاج إلى معرفته كل مستخدم. مجلة The Guardian. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من:
http://www.guardian.co.uk/technology/gamesblog/2011/apr/27/psn-security-advice

100 لمزيد من المناقشات الموسعة حول أنواع تقنية برامج مراقبة الحزم أنظر مويلر إم (2011) (Mueller M). تقنية DPI من منظور دراسات إدارة الإنترنت: مقدمة. جامعة سيراكيوز. تم الاسترجاع من
http://dpi.ischool.syr.edu/Technology_files/WhatisDPI-2.pdf

101 مويلر إم. (2011.) (Mueller M). تقنية DPI من منظور دراسات إدارة الإنترنت: مقدمة. جامعة سيراكيوز. تم الاسترجاع من http://dpi.ischool.syr.edu/Technology_files/WhatisDPI-2.pdf

القانونية.[102] كما أنها لم تفيد الفهم العام لتقنية برامج مراقبة الحزم، التي ارتبطت منذ ذلك الحين ارتباطا وثيقا بانتهاكات الخصوصية في أي جدل عام. وفي سياق الاحتجاجات الشعبية العارمة في جمهورية إيران الإسلامية ومنطقة الشرق الأوسط وشمال إفريقيا في عام 2009، و2010 و 2011، ذكرت تقارير واسعة النطاق أن تقنية برامج مراقبة الحزم (DPI) كانت تستخدمها الحكومة في تتبع ومراقبة مواطنيها.[103]

ومنذ هذه التقارير الأولية، استمر نشر أدلة موثقة جيدا تربط بين هذه التقنية وبين بعض أنظمة المراقبة في منطقة الشرق الأوسط وشمال إفريقيا. وما وراء هذه المنطقة، تعتبر هذه التقنية جزء شائع من أنظمة المراقبة الحكومية، والتي تسمى أحيانا باسم «الاعتراض المشروع.» فهي تساعد على رؤية جميع المعلومات غير المشفرة التي تمر عبر شبكات الاتصالات أمام مشغلي المعدات، مما يسمح لهم بتخزين المعلومات الموجودة في الشبكة وفي بعض الحالات تعديلها.[104]

من الاستخدامات الأخرى الشائعة لتقنية برامج مراقبة الحزم (DPI) هو تصنيف المستخدمين بملفات تعريف على شبكات الاتصالات، وذلك من الواضح لأغراض تجارية، وإن كان من غير الواضح مدى شمولية هذه الملفات التعريفية. ولكن في بعض الحالات يمكن فقط استخدام هذه الملفات التعريفية لأغراض الدعاية لاستهداف مستخدمي الشبكة بالإعلانات ذات الصلة. ومن الأشكال الأخرى المتعدية على الخصوصية باستخدام تقنية برامج مراقبة الحزم (DPI) تصفية المحتوى على الإنترنت، لأنه يعتبر غير قانوني في العادة. وفي كثير من الحالات يسمح هذا بمراقبة المستخدمين الذين يرغبون في الوصول إلى المحتوى بعد تصفيته.

ويمكن استخدام هذه التقنية بشكل خاص في إدارة عرض النطاق الترددي من قبل مزودي خدمات الإنترنت لمنع الرسائل غير المرغوب فيها على مستوى الشبكة وحماية مزودي خدمات الإنترنت من أنواع معينة من هجمات الإنترنت. وهنا لا تعتبر «سيئة بطبيعتها» كما يدعي البعض، ولكنها تطرح تساؤلات أخلاقية كبيرة عند تنفيذها. وقد حاول بعض المزودين التخفيف من هذه المشاكل من خلال تطوير أنواع «خصوصية حسب التصميم» لتقنية برامج مراقبة الحزم (DPI)، وإن كانت هذه التطورات لا تزال في مراحلها الأولى.[105] وفي سياق المسائل الأخلاقية المتصلة بالخصوصية، نجد أن وضع هذه التقنية كتقنية عامة لمراقبة الاتصالات قد يمكن إساءة استخدامها في سياقات مختلفة. وبعد نضوج صناعة هذه التقنية، يبقى أن نرى كيف يمكن للشركات المختلفة داخلها أن تحدد موضعها ضمن طرق إساءة استخدام هذه التقنية وكيف يمكن للتقارب المحتمل بين الاستخدامات المختلفة لها أن تؤثر على الصناعة ككل.

---

102 اللجنة الأوروبية. (2010). جدول الأعمال الرقمي. اللجنة تحيل المملكة المتحدة إلى المحكمة بشأن حماية الخصوصية والبيانات الشخصية [1215/IP/10]. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011 من: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1215

103 أنظر سيلفر في وإلجين، بي. (2011) (Silver, V., & Elgin, B.). التعذيب في البحرين يصبح عادة بمساعدة نوكيا سيمنز (Nokia Siemens). بلومبرج. تم الاسترجاع في 28 أغسطس 2011، من: http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html وسون، بي وكوكر إم.
(2011) (Sonne, P., & Coker, M.). الشركات الأجنبية ساعدت القذافي على التجسس على الليبيين. مجلة Wall Street Journal. تم الاسترجاع في 23 سبمتبر 2011، من: http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html

104 اللجنة الأوروبية. (2010). جدول الأعمال الرقمي. اللجنة تحيل المملكة المتحدة إلى المحكمة بشأن حماية الخصوصية والبيانات الشخصية [1215/IP/10]. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011 من: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1215

105 هذه المعلومات قائمة على المقابلات الشخصية التي أجراها المؤلف في يوليو 2011.

4.3.2. انتشار تكنولوجيا تحديد المواقع الجغرافية: خطر ناشئ ضد الخصوصية على الإنترنت

ظلت بيانات الموقع الجغرافي على مر التاريخ جزءاً لا يتجزأ من شبكة الإنترنت. وقد استخدمت الأنظمة ذات القدرة على تحديد موقع مستخدمي الإنترنت بدرجة عالية نسبياً من الدقة في أغراض الإعلانات والأغراض القانونية على حد سواء. وتوفر هذه الخدمات الموقع الجغرافي لعناوين بروتوكول الإنترنت (IP) الخاص بالمستخدمين وتسمح لمزودي خدمات الإنترنت بوضع تقدير دقيق نسبياً حول الموقع الذي يتواجد فيه المستخدم، وربما المدينة في كثير من الحالات. ومع ارتفاع نسبة استخدام الإنترنت وزيادة استخدام البيانات على الإنترنت، ارتفعت كذلك دقة هذه الخدمات وبالتالي زادت قدرة المواقع الالكترونية والوسطاء على تحديد الموقع الجغرافي لمستخدمي الإنترنت.

وعلى الرغم من ذلك، تشير التطورات التقنية في الأجهزة المتصلة بالإنترنت إلى أنه أصبح لدى العديد من مستخدمي الإنترنت الآن نظام تحديد المواقع العالمي، وهي تقنية تتميز بالدقة العالية جداً، مما يسمح بتحديد تفاصيل الموقع المادي لمستخدم الإنترنت ضمن بضعة أمتار. وفي نفس الوقت تم تضمين هذه التقنية في العديد من الأجهزة المختلفة دون معرفة المستخدمين في العادة للعواقب التي قد تنتج عن تفعيل أو إيقاف هذه الخاصية، وتتصل هذه التطبيقات أو البرامج بمعلومات الموقع المحددة بنظام تحديد المواقع العالمي (GPS).

إن تقديم معلومات نظام تحديد المواقع العالمي (GPS) يقوم من خلال العديد من نماذج الأعمال عبر الإنترنت. ويتم تشجيع مستخدمي FourSquare والفيسبوك (Facebook) لتقديم معلومات عن مكانهم عند زيارة الموقع، وتكون هذه خاصية اجتماعية في المقام الأول. ويشيع كذلك في أشكال أخرى من الشبكات الاجتماعية مثل "CouchSurfing"، حيث يكون الموقع المتوفر هنا أقل دقة من الموقع المتوفر على FourSquare والفيسبوك (Facebook). ومن الجدير أن هذه كلها مواقع تواصل اجتماعي في صورة أو بأخرى، ولكن بالنسبة لموقع FourSquare وCouchsurfing ربما يمكن القول بأن تقديم معلومات المكان هي بطبيعتها جزء من مفهوم الشبكة. ويتوقع المستخدمون عند الانضمام إلى هذه الشبكات الاجتماعية مشاركة معلوماتهم، بل ربما ينضمون لهذا السبب تحديداً؛ ولكن يبدو هذا الرأي أقل وضوحاً في حالة الفيسبوك (Facebook).

تثير أنظمة المواقع الجغرافية على ما هو واضح بعض الإشكاليات المتعلقة بموافقة المستخدم وتحكمه في بياناته الشخصية الخاصة بموقعه الجغرافي. حيث لا يستطيع المستخدم إحكام السيطرة الكاملة الفعلية على البيانات الخاصة به وأشكال معالجتها، مما يصعب من وجود الموافقة المستنيرة. وعلاوة على ذلك، تتم معالجة بيانات الموقع الجغرافي بكثافة ويمكن الحصول عليها – كما نوقش أعلاه – من معلومات أخرى يوفرها المستخدم دون معرفته أو موافقته لهذه العملية. كما تتميز أنظمة تحديد المواقع العالمية (GPS) المدمجة في الأنظمة اليدوية بدقتها العالية التي تفوق تحديد الموقع الجغرافي باستخدام أبراج الاتصالات النقالة، وتوفر صورة أكثر دقة لتحركات الفرد.

ويمكن عندئذ استخدام بيانات الموقع الجغرافي التي تم جمعها بهذه الطريقة في إنشاء ملفات تعريف لحركة الأفراد. ومن الأمثلة الأكثر إثارة في الآونة الأخيرة مالتي سبيتز (Malte Spitz)، وهو سياسي ألماني مناصر لحماية البيئة رفع دعوى قضائية ضد شركة تزويد هواتف نقالة للوصول إلى بياناته الشخصية حتى يرى ما يعرفونه عن تحركاته. وقد نشرت المعلومات التي تلقاها فيما بعد في إحدى الصحف الألمانية وأصبحت تمثل ملفاً كاملاً عن تحركاته خلال فترة حياته، ونشر بعضها على الإنترنت لإظهار حجم المشكلة.[106] ومن الواضح أنه بينما تظل تقنية تحديد المواقع الجغرافية والخدمات المتصلة بها في تطور مطرد، يظل من الصعب ترقب مدى تأثيرات تطوراتها المستمرة على الخصوصية على شبكة الإنترنت. ولكن توحي نظرة

---

[106] بيرمان، كاي (2011) (Biermann, Kai.) «حماية البيانات: الخيانة بفعل بياناتنا الخاصة». ZEIT Online. تم الاسترجاع في 1 مارس/ آذار2012 http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz

متوجسة على بعض المسائل التي تستخدم من أجلها هذه التقنية إلى إنه من المستبعد وجود «حلول سريعة» للعديد من المسائل الإشكالية المرتبطة بخصوصية المواقع الجغرافية – رغم أن مسألة المواقع الجغرافية هي مسألة ليست بالقديمة.

5.3.2. معالجة البيانات والتعرف على الوجه

«برزت تقنية التعرف على الوجه (FRT) لتمثل حلاً جذاباً في تلبية الكثير من الاحتياجات المعاصرة للتعرف على الهوية والتحقق من صحتها، حيث جمعت بين ما وعدت به النظم الأخرى للتحقق من الهوية من خلال السمات البيولوجية، والتي تحاول ربط الهوية بسمات مميزة من الجسد لدى لكل فرد، والوظيفة الأكثر انتشاراً من أنظمة المراقبة المرئية».[107]

10) إعادة معالجة الوجه

بهدف إظهار ما تنطوي عليه عملية مشاركة المعلومات علنا من مخاطر، قام مجموعة من الفنانين بتحميل ما يزيد على مليون صورة متوفرة بشكل عام على موقع الفيسبوك (Facebook)، ومعلومات شخصية وعلاقات مرتبطة بها.[108] ثم استخدموا هذه المعلومات في تصنيف الوجوه و(إعادة) تصنيفها على موقع آخر. وعلى الرغم من أن هذه المبادرة هي عبارة عن مشروع عام يهدف إلى رفع مستوى الوعي حول مرونة وقابلية تكرار البيانات العامة، إلا أن هناك العديد من «Internet Bots“ – أو بوتات الإنترنت – الأخرى التي تمضي الوقت في «تجريف» مواقع الإنترنت سراً واستخدام هذه المعلومات في تغذية قواعد بيانات خاصة. وهذا يعني أيضاً أن الخيارات الطارئة لنشر المعلومات من قبل مستخدمي الإنترنت قد ينتج عنها عواقب لا يمكن تفاديها، مع "سرقة" البيانات الخاصة من الموقع الذي نشرت عليه ونسخها في أقل من ثانية. وينتج عن تدني مستوى الوعي لدى المستخدمين بشأن المدى المحتمل لخيارات خصوصيتهم وعدم السيطرة على المعلومات الخاصة بهم بمجرد إتاحتها بشكل علني (لأي سبب كان) آثار سلبية وخيمة على خصوصية المستخدم على الإنترنت.

وبرغم كثرة الجدل في السنوات الأخيرة حول تأثير تقنية التعرف على الوجه على خصوصية الفرد، يتعين دراسة هذا التأثير من منظور أوسع. ففي حين أدخلت جوانب حديثة ضمن هذا الجدل، إلا إن هذه التقنية في كثير من النواحي تمثل شكلاً جديداً من أشكال معالجة البيانات والتعرف على الهوية.

وثمة الكثير من الأسباب وراء انطواء معالجة البيانات على مثل هذه التأثيرات المهددة لخصوصية الأفراد على الإنترنت. أول هذه الأسباب أنها تعيد إنشاء سياق جديد للبيانات وتعالجها بشكل لم يكن مطلوباً أو متوقعاً أو حتى متصوراً. ففي السياق المختلف، قد تحمل البيانات التي تمت معالجتها معنى مختلفاً تماماً. مما قد يؤدي بمعالجات البيانات بالفعل إلى معالجة معلومات عن حياة الفرد الشخصية هو على علم بها.

وهنا تقوم تقنية التعرف على الوجه بمعالجة ما كان في السابق عبارة عن معلومات محددة للهوية ضمن البيانات الشخصية. حيث بدأت القوة المتزايدة لتقنية التعرف على الوجه وعلى نحو متزايد في أن تزيد من ربط الوجه بمحدد هوية فريد يمكن ربطه من خلال ملفات التعريف الخاصة والعامة على شبكة الإنترنت (أنظر المربع لمزيد من التفاصيل). ولقد أصبحت السمة الأساسية لربط البيانات وتحديد الهوية. ونتيجة لذلك

---

107 إنتروما إل دي، ونيسينباوم إتش إف (2009) (Introna, L. D., & Nissenbaum, H. F.). تقنية التعرف على الوجه: دراسة استقصائية حول مسائل السياسة والتنفيذ. SSRN eLibrary. SSRN.

108 سيريو بي و لودوفيكو إيه (Cirio, P., & Ludovico, A.) (2011). Face-to-Facebook. Face-to-Facebook. تم الاسترجاع من: www.face-to-facebook.net/theory.php

بدأ المستخدمون في إدراك أن المعلومات التي توقعوا أنها مجهولة قد تكون مربوطة بملفاتهم الشخصية عبر الإنترنت أو تكون قابلة للبحث تحت اسمهم. وفي عالم أصبحت فيه عدسات الكاميرا في تزايد مستمر، قد ينتج عن هذا آثار مروعة على حرية التعبير، وتأثيرات سلبية مماثلة على الخصوصية.[109]

كما تم استخدام تقنية التعرف على الوجه من قبل أجهزة تنفيذ القانون كجزء من عمليات المراقبة في الفعاليات العامة الكبيرة، مثل Superbowl 2001 في ولاية فلوريدا، الولايات المتحدة الأمريكية.[110] ومع استمرار البلاغات المتعلقة بهذه التقنية منذ ذلك الحين، هناك ما يدعو للاعتقاد بأن أجهزة تنفيذ القانون والسلطات العامة الأخرى تستخدم تقنيات مماثلة للتعرف على الوجه على شبكة الإنترنت. وعلى الرغم من اتساع نطاق الشكوك المتعلقة بمدى فعالية تقنية التعرف على الوجه كأداة من أدوات تنفيذ القانون، إلا أن الاستثمار المتواصل في هذه التقنيات من قبل السلطات العامة في جميع أنحاء العالم يوحي إلى أنه من المتوقع تطور هذه التقنية بشكل سريع في المستقبل القريب.[111]

وثمة تطور آخر له تأثيرات كبيرة على الخصوصية في هذا السياق، ألا وهو نقل كميات كبيرة من البيانات الشخصية بين القطاع العام والخاص. إذا تقوم السلطات العامة على نحو متزايد بطلب البيانات الشخصية التي تمت معاجلتها من جديد من جانب القطاع الخاص (مثل ملفات تعريف البحث أو تاريخ شبكات التواصل الاجتماعي).[112] وفي الوقت نفسه يقوم القطاع العام بتشارك البيانات الشخصية، مثل "ملفات المخابرات" الفردية التي أعيدت معالجتها، مع القطاع الخاص على نحو متزايد.[113] هذا التبادل للبيانات الشخصية التي تمت معالجتها تمثل خطراً كبيراً لسيطرة الفرد على المعلومات الشخصية الخاصة به. فلا يتوقع مستخدمو شبكات التواصل الاجتماعي أن يتم تشارك بياناتهم التي أدخولها على الشبكة، أو أن تخزن تحركاتهم لدى مزود خدمة الهاتف النقال مع أجهزة تنفيذ القانون. ولا يتوقع عادة المواطنون أن يتم تشارك المعلومات التي جمعتها أجهزة الاستخبارات أو أجهزة تنفيذ القانون بشكل طبيعي مع معنيين من القطاع الخاص.

فلقد باتت مسائلة تشارك المعلومات الشخصية في كلا الاتجاهين أمراً شائعا على شبكة الإنترنت، بل بدا من الممكن دمج بنية المراقبة العامة مع بنية المراقبة الخاصة. وتمثل مراكز تبادل المعلومات الاستخباراتية مثل PNR وSWIFT، وتشريعات الاحتفاظ بالبيانات بشكل عام، أمثلة قليلة فقط على جمع القطاع الخاص للبيانات ثم استخدامها من جانب القطاع العام أو العكس. وهنا، يزيد التداخل بين أنظمة الخصوصية في القطاع الخاص والعام من صعوبة موافقة الأفراد على استخدام البيانات من قبل أطراف ثالثة، أو معرفتهم كيفية وظروف تخزين بياناتهم، ناهيك عن إمكانية سحبهم للموافقة من التخزين الرقمي للبيانات الخاصة بهم.

وفي هذا السياق أصبحت تقنية معالجة البيانات والتعرف على الوجه جزءاً من بنية المراقبة التحتية الأوسع، مما يهدد الأسس التي تقوم عليها الخصوصية، والدافع في ذلك هو رغبة القطاع العام في معرفة المزيد عن

---

109 بادانيا، إس. وجريغوري، إس. وألبيردينغك-ثيجمن واي. ونوناز بي (2011) ,.Padania, S., Gregory, S Alberdingk-Thijm, Y., & Nunez, B. تقرير انتشار الكاميرات في كل مكان 2011. تم الاسترجاع من: //:http www.witness.org/cameras-everywhere/report-2011

110 المنظمة الدولية لحماية الخصوصية (2006) .(Privacy International). المنظمة الدولية لحماية الخصوصية (Privacy International) (2006) – ملخص تنفيذي. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من https://www.privacyinternational.org/article/phr2006-executive-summary

111 مركز معلومات الخصوصية الالكترونية. (2011). التعرف على الوجه. (EPIC). تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من: /https://epic.org/privacy/facerecognition

112 جوجل. (2011). تقرير شفافية جوجل. جوجل. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011 من: //:https www.google.com/transparencyreport/

113 كارتر دي إل. وكارتر جي جي (2009) (.Carter, D. L., & Carter, J. G). عملية دمج المخابرات لتنفيذ قانون الدولة والقانون المحلي والقبلي. العدالة الجنائية والسلوكيات، 36 (12)، 1323-1339.

المواطنين، والسوق الخاصة التي سرعان ما نشأت لتلبية هذا المطلب.[114] وفي الختام، يبدو من المعقول أن نشير إلى حدوث «انفجار في نشر الصور، في مجالات من تشارك الصورة إلى المراقبة والتصوير الطبي، مع زيادة في المقابل في إمكانية الاستخدامات المعتدية على الخصوصية لتلك الصور. وحتى الآن، كانت الضوابط المفروضة على عمليات التعدي على الخصوصية التي جلبتها هذه التقنية محدودة للغاية».[115]

6.3.2. تقنية مراقبة الإنترنت

عند الانتقال من معالجة البيانات والتعرف على الوجه إلى السوق للتعرف على هذه المعدات نجد أن أكبر الأخطار التي تهدد الخصوصية على الإنترنت تنبثق عن انتشار صناعة مراقبة الإنترنت. فعلى الرغم من أن مناقشة تقنية مراقبة الإنترنت تأتي في سياق تقنية التفتيش العميق للحزم (DPI)، إلا إن أنواع التقنيات المستخدمة في تكنولوجيا مراقبة الإنترنت هي أوسع بكثير. فالتقنيات المستخدمة تتراوح بين برامج مثبتة على أجهزة الكمبيوتر الفردية من قبل أجهزة تنفيذ القانون مثل «حصان طروادة» (Trojan Horse)، وأجهزة الرصد التي تلحق بأنظمة الحوسبة الشخصية أو الأجهزة الإلكترونية ووصولاً إلى تقنيات المراقبة التي تلحق بشبكات الاتصالات التي تتصل بها الأجهزة.

ومن المخاوف الخاصة المتعلقة بالخصوصية تلك التقنيات التي تسعى إلى تسخير البيانات الشخصية التي قام مستخدمو الإنترنت بتحميلها وتنظيمها، وبالتالي معالجة كمية هائلة من المعلومات الشخصية بشكل طبيعي. فالتقدم في مجال قوة المعالجة الحاسوبية تعني بأن تقنية مراقبة الإنترنت قادرة على فهرسة بيانات المستخدم الشخصية وربطها بإشارات مرجعية وتكوين ملفات تعريفية لها. ولقد توسعت تكنولوجيا مراقبة الإنترنت من حيث التنوع والنطاق والاستخدام بشكل كبير منذ بدايات الإنترنت العامة.[116] ويتم توفير هذه التقنيات في العادة للحكومات والشركات الكبرى في جميع أنحاء العالم، بغض النظر عن سوء استخدام المعلومات الخصوصية والمخاوف المتعلقة بحقوق الإنسان. والنتيجة هي وجود سوق لهذه التقنيات تتنافس فيه الشركات على قديم أكثر التقنيات اختراقاً للخصوصية. وليس للشركات العاملة في هذه السوق أية مصلحة تذكر في حماية خصوصية الأفراد؛ بل تتركز مصلحتها الواضحة في الكشف عن خصوصية المستخدم إلى أقصى حد ممكن.

كما زادت التجارة الدولية في تكنولوجيا المراقبة والخدمات من نقل البيانات الشخصية عبر شبكات الاتصالات. حيث إن معظم تقنيات المراقبة الحديثة مصممة «للاتصال بمصدرها»، أو "الإبلاغ إلى المصدر" أو نقل نتائجها بأي طريقة إلى مشغليها. وبما أن المشغلين والفنيين نادراً ما يتواجدون في نفس الموقع الفعلي كما هو الحال في معدات المراقبة، يتعين نقل المعلومات الشخصية التي يتم جمعها بأجهزة المراقبة عبر شبكات الاتصالات إلى المشغلين. وفي الوقت نفسه يمكن للعديد من تقنيات مراقبة الإنترنت تحديث نفسها عبر شبكات الاتصالات ويمكن أن توفر إمكانية الوصول عن بعد لمزود تقنيات المراقبة. هذه القدرة للوصول عن بعد ونقل البيانات الشخصية لها تهديدات واضحة على خصوصية البيانات الشخصية. وثمة العديد من الحالات الموثقة جيداً عن استغلال أطراف ثالثة لتقنيات المراقبة (يورد المربع أدناه مثالاً على ذلك).

---

114 سيلفر في وإلجين بي (2011) (.Silver, V., & Elgin, B). التعذيب في البحرين يصبح عادة بمساعدة نوكيا سيمنز (Nokia Siemens). بلومبرج. تم الاسترجاع في 28 أغسطس/ آب 2011، من: http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html

115 سينيور إيه وبانكاني إس. (2011). حماية الخصوصية والتعرف على الوجه. في إس زاد لي و كي جاين (S. Z. Li & A. K. Jain) (محررون). دليل التعرف على الوجه. Springer

116 كينج إي (2011). ردنا على استشارة الاتحاد الأوروبي بشأن مشروعية استيراد تكنولوجيا المراقبة والرقابة. المنظمة الدولية لحماية الخصوصية (Privacy International). تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من https://www.privacyinternational.org/article/our-response-eu-consultation-legality-exporting-surveillance-and-censorship-technology

وعلاوة على ذلك، إن إضافة تقنيات المراقبة للأجهزة والأنظمة والشبكات التقنية تضيف طبقة أخرى إلى نقاط الضعف. وتكون نقاط الضعف هذه واضحة عند تصميم تقنية المراقبة لاستخراج وإعداد البيانات الشخصية للمشغلين. ومن ثم يمثل حصول الطرف الثالث على أنظمة المراقبة تهديداً أكبر بكثير على الخصوصية من الحصول على الأنظمة أو الأجهزة أو الشبكات الفعلية التي يجري مسحها. وكما سنناقش في الفصل 3 بمزيد من التفصيل، ثمة عدد محدود من الحالات التي يمكن أن يبرر فيها استخدام تقنيات المراقبة في إطار قانوني واضح يستند إلى حقوق الإنسان وسيادة القانون. ولكن حتى في هذه الحالات تعتبر تقنيات المراقبة في أساسها متعدية على الخصوصية، مما يجعل من استخدامها تهديداً واسعاً جداً على الخصوصية على شبكة الإنترنت.

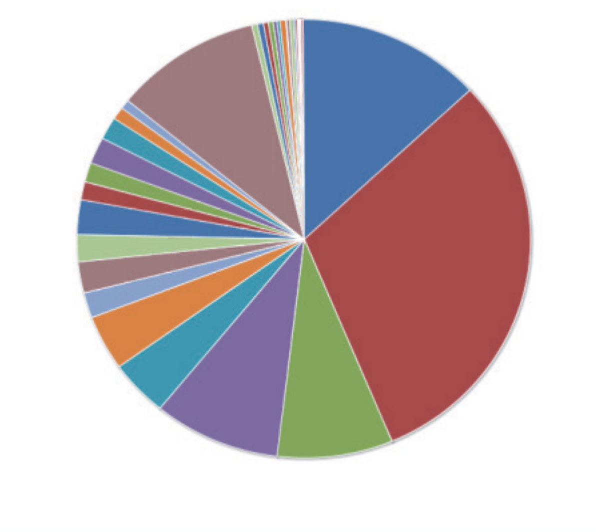
11) نشر سجلات المراقبة

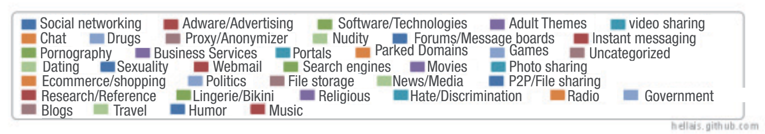
في أكتوبر/ تشرين الأول من عام 2011 أصدرت مجموعة Telecomix الناشطة على الإنترنت ملفات سجلات كثيرة من معدات مراقبة الإنترنت في الجمهورية العربية السورية.[117] وقدمت بيانات المراقبة المنشورة كذلك صورة غير عادية من داخل نظام مراقبة الإنترنت. حيث عرضت رؤية متعمقة حول كيفية محاولة المستخدمين بشكل فعال وغير فعال في حماية خصوصيتهم وعدم الكشف عن هويتهم باستخدام أدوات الإنترنت. وتصنف المستخدمين على شبكات التواصل الاجتماعي إلى فئة تقوم بالتسوق، وثانية تبحث عن إعلانات، وثالثة تستخدم محركات البحث ومواقع مشاركة الفيديو أو الصور. وأكثر ما تقدمه هو رؤية متعمقة داخل القوة الخارقة لمعدات المراقبة المصممة للتعدي على الخصوصية الشخصية بما يتجاوز كل حدود الفضاء الخاص أو سرية الهوية أو الكرامة الإنسانية. ويتم تسجيل النشاط الفردي يوماً بيوم وتصنيفه، ثم تعرض تعبيراتهم عن آمالهم وأحلامهم الشخصية غير الموجهة إلى الرأي العام. ويمكن التعرف على نظرة عامة موجة أدناه.

---

117 فالينتينو-ديفريس، جي. سون بي؛ ومالاس إن (2011)، (Valentino-Devries, J., Sonne, P., & Malas, N.). شركة بلو كوت الأمريكية تقر باستخدام سوريا لعتادها في الرقابة على الإنترنت في خضم الربيع العربي. مجلة وول ستريت. تم الاسترجاع في 13 ديسمبر/ كانون الأول 2011، من http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

الشكل 2: استعراض سجلات المراقبة[118]





118 فيلاستو إيه (.Filasto, A)(2011). تشير ملفات أجهزة بلو كوت إلى مستويات الرقابة في سوريا. تم الاسترجاع في 12 ديسمبر/ كانون الأول 2011 من /http://hellais.github.com/syria-censorship

3. البيئة القانونية والتنظيمية الدولية لحماية الخصوصية

إن الحق في الخصوصية هو من الحقوق القديمة، وقد وردت الإشارة إليه في مختلف الأعراف الدينية – بما فيها اليهودية والمسيحية والإسلامية – فضلاً عن الإغريق والصين في عصورها القديمة. وكان لبعض أشكال حماية الخصوصية وجود في انكلترا في زمن يعود إلى 1361 عندما صدر قانون لحماية الخصوصية باسم Justices of the Peace Act يجرم التنصت واختلاس النظر على محارم الغير.[119] وحظيت الخصوصية بحماية مثل أي حق من حقوق الإنسان الدولية منذ البداية، فكان لها نصيب من أحكام الإعلان العالمي لحقوق الإنسان (UDHR)،[120] وكذلك العهد الدولي الخاص بالحقوق المدنية والسياسية (ICCPR).[121]

وفي الوقت ذاته، تبين أنه من الصعب تحقيق توافق في الآراء على محتوى معين لهذا الحق، وبدا من الواضح أنه يحمل في جوهره مفهوماً محدداً للحق في عدم التعرض للتدخل الخارجي، وهو ما نتج عنه تعاريف متباينة لكل من أراد أن يدلي بدلوه في تعريف هذا الحق. فجاء التقرير الصادر عن حكومة المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية بشأن الخصوصية، المعروف باسم تقرير كالكوت (Calcutt) ليصرح عن عجز المؤلفين عن التوصل إلى «تعريف مرض للجميع» بشأن الخصوصية.[122]

أما وارين وبرانديز (Warren and Brandeis) في الورقة المواضعية التي أعدت حول الخصوصية في العام 1890 فقد عرفا الخصوصية على أنها "الحق في أن يخلى المرء وشأنه".[123] ثم حددت القرارات الصادرة عن كبرى محاكم الولايات المتحدة الأمريكية أربعة أنواع مختلفة من الحق في الخصوصية: التدخل غير المبرر في عزلة الغير، استغلال اسم المرء أو شكله، الدعاية التي تسليط الضوء الزائف على المرء والدعاية غير المبررة لحياة المرء الخاصة.[124] وعرفت المحكمة الدستورية في جنوب أفريقيا مؤخراً الخصوصية على أنها «حق الشخص في أن يعيش حياته كما يشاء».[125] وعرفتها المحكمة العليا الكندية بأنها "النطاق الضيق للاستقلالية الشخصية الذي تتم في إطاره تقرير الاختيارات الخاصة بطبيعتها".[126] وقد تجنبت المحكمة الأوروبية لحقوق الإنسان تعريف الخصوصية بقولها: «إن المحكمة لا ترى من إمكانية أو ضرورة في محاولة وضع

---

119 مركز معلومات الخصوصية الالكترونية والمنظمة الدولية لحماية الخصوصية (Privacy International)، الخصوصية وحقوق الإنسان 2006: دراسة استقصائية دولية لقوانين الخصوصية وتطوراتها (مركز معلومات الخصوصية الالكترونية المنظمة الدولية لحماية الخصوصية (Privacy International: 2007)، ص. 5.

120 قرر الجمعية العامة للأمم المتحدة رقم 10 ،(III)217A ديسمبر/ كانون الأول 1948.

121 اعتمدته الجمعية العامة للأمم المتحدة بموجب القرار رقم 16 ،(XXI) 2200A ديسمبر/ كانون الأول 1966، ودخل حيز النفاذ في 23 مارس/ آذار1976.

122 كالكوت دي (Calcutt, D.) وآخرون (1990). تقرير اللجنة المعنية بالخصوصية والمسائل ذات الصلة، الرئيس دافيد كالكوت، مستشار الملكة، لندن: HMSO (المقترح الرسمي رقم 1102)، ص 7.

123 «الحق في الخصوصية» (1890) 4 استعراض القانون لدى جامعة هارفارد 193، صفحة 195.

124 أنظر ليك ضد وال مارت سلورز إنك (Lake v. Wal-Mart-Stores Inc.) ،30 يوليو 1998، محكمة مينيسوتا العليا، C7-97-263. أنظر أيضاً، البيان المكرر (الثاني) للأضرار، § 1977) 652B-E)

125 إن إم وآخرون ضد سميث وآخرون (NM and Others v. Smith and Others)، 2007 (7)، BCLR 751. الفقرة 33.

126 جودباوت ضد لونجويل (Godbout v. Longueuil) (مدينة) [1997] 3 SCR 844، الفقرة 97.

تعريف جامع لمفهوم "الحياة الخاصة».[127] وفي قضية Ponzetti de Balbín, Indalia vs Editorial Atlàntida S.A.، عولت المحكمة العليا الأرجنتينية أيضاً على تعريف فضفاض للغاية للخصوصية.[128]

هذا ومن الواضح جداً أن لمضمون الحق عنصر موضوعي، وذلك بقدر ما قد يقوم المرء بتناول أمر من الأمور على أنه أمر عام بطبيعته، فيقدمه بهذه الصورة أو ربما يتنازل عن بعض أجزاء من خصوصيته. وبالتالي، يعتبر الميول الجنسي للمرء من خصوصياته، ولكن يمكن للمرء أن يجعله أمراً عاماً مراراً وتكراراً من خلال الدعوة إليه. وهنا قد يتصادم هذا الحق مع الحقوق الشخصية الأخرى، مثل الحق في حماية السمعة أو في حرية التعبير، والتي تميزها حدود أكثر وضوحاً أو أكثر موضوعية. وقد تدخل بعد ذلك في إطار ما يسمى بـ «المواد الإباحية الشديدة» (hard core pornography) التي نوه إلى صعوبة تعريفها القاضي ستيوارت (Stewart) لدى المحكمة العليا الأمريكية، وقال «لكنني أعرفها عندما أراها».[129] وتتفاقم مشكلة التعريف بسبب ما لمفهوم المصلحة العامة من دور في هذا الشأن، والذي يصعب جداً وضع تعريف دقيق لها هي الأخرى، وذلك في وضع تعريف لما تعنيه حماية نطاق الخصوصية. علما بأن انتفاء التعريف زاد من صعوبات تطبيق وتنفيذ الحق في الخصوصية.

وتعتبر فكرة حماية البيانات، والتي لها أهمية خاصة بالنسبة لمفهوم الخصوصية وشبكة الإنترنت، من الأفكار الحديثة جداً، وقد نشأت جذورها أساساً في التوجه الزائد نحو جمع البيانات الشخصية عن الأفراد من قبل الحكومة. ثم كان ظهور أجهزة الحاسوب (الكمبيوتر) ثم من بعدها الإنترنت بمثابة الدفعة القوية التي تبلور على إثرها مفهوم حماية البيانات. فأول قانون تقنن في شأن حماية البيانات قد أشارت أحكامه إلى أراضي (أو مقاطعة) هيس (Hesse) في ألمانيا في العام 1970، ويعود الفضل إلى السويد التي اعتمدت أول قانون وطني في عام 1973.

إن المفهوم الأساسي وراء حماية البيانات هو أن للأفراد الحق في السيطرة على جمع واستخدام البيانات التي قد تحدد هويتهم من خلالها (البيانات الشخصية). كما تخضع حماية البيانات، مثلها مثل الخصوصية، إلى قيود معينة منها تحقيقات الشرطة في الجريمة كقيد من القيود الواضحة. وقد تقارن حماية البيانات مع حماية الخصوصية من حيث وضوح المفاهيم الأساسية التي تقوم عليها وضوحاً كبيراً وحشدها لتوافق واسع، رغم بعض الاختلافات المهمة.

من القضايا المهمة لخصوصية الإنترنت بشكل عام تلك العلاقة الدقيقة القائمة بين الخصوصية وحماية البيانات، أو بعبارة أخرى مدى ضمان مبادئ حماية البيانات كجزء من الحق الراسخ للإنسان في الخصوصية؛ ومن الواضح أن ثمة اختلاف بين هذين الأمرين، وأن حماية البيانات لا تندرج تماماً ضمن مفهوم الخصوصية.[130] ولكن يمكن أن تستمد أهمية مبادئ حماية البيانات مباشرة من حق الإنسان في الخصوصية، وهذا يلقى ما يدعمه في الفقه الدولي. وهذا أقل وضوحاً من المبادئ الأخرى، وبالتأكيد من الأنظمة التي تتبع في توفير حماية ملموسة للبيانات.

---

127 نيميتز ضد ألمانيا Niemietz v Germany 16 ديسمبر/ كانون الأول 1992، 16 EHRR 97. الفقرة 29. أنظر أيضاً وركمان آر (Workman, R.) الذي كتب في 1992 يقول: "لقد أدى التعريف الثابت «للخصوصية» إلى تضليل المعلقين". "التوازن بين الحق في الخصوصية والتعديل الأول" (1992) 29 استعراض القانون بجامعة هوستن 1059، ص. 1063.

128 تقرر في 11 ديسمبر/ كانون الأول لعام 1984، محكمة العدل العليا للأمة (CS)، الفقرة 8، متوفر على: http://www.fallodelderecho.com.ar/jurisprudencia-argentina/ponzetti-de-balbin

129 جاكوبيليس ضد أوهايو (Jacobellis v. Ohio، 378 الولايات المتحدة. 184 (1964)، في 197.

130 اعترافاً بذلك، ورد ضمن أحكام ميثاق الحقوق الأساسية للاتحاد الأوروبي حماية الخصوصية وحماية البيانات (أنظر الحاشية رقم 208). مشاريع قانون اللجنة الأوروبية الجديدة لتنظيم حماية البيانات تعكس أيضاً هذه الفكرة، إذ تقرر ما يلي: «ترتبط حماية البيانات بروابط وثيقة باحترام الحياة الخاصة والأسرية». أنظر الحاشية 217. صفحة 7.

1.3. الحماية الدولية للخصوصية والبيانات الشخصية

1.1.3. الخصوصية

1.1.1.3. المعايير العالمية

تحظى الخصوصية بالحماية المباشرة والصريحة بموجب القانون الدولي لحقوق الإنسان، فقد نصت المادة 12 من الإعلان العالمي لحقوق الإنسان على ما يلي:

(1) لا ينبغي أن يتعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات.

(2) وقد أضفيت الحماية القانونية الرسمية على هذا بموجب المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية، التي تنص على:

لا ينبغي أن يتعرض أحد لتدخل تعسفي أو غير قانوني في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه وسمعته.

لكل شخص الحق في حماية القانون من مثل هذا التدخل أو المساس.

هذان التعريفات متشابهان، ولكن مع بعض الاختلافات المهمة. حيث إن الإعلان العالمي لحقوق الإنسان يحمي فقط من التدخل التعسفي، وليس التدخل غير المشروع، في الخصوصية. وفي الواقع قد يكون لهذا الاختلاف أهمية محدودة لأن التدخل غير المشروع سيعتبر دائماً تدخلاً تعسفياً. وبخصوص الشرف والسمعة، يقتصر العهد الدولي الخاص بالحقوق المدنية والسياسية على الحماية من المساس الهجمات المحظورة، بينما يكفل الإعلان العالمي لحقوق الإنسان الحماية ضد كل هذه الهجمات. وقد يكون لهذا أهمية أكثر من حيث طبيعته، على الرغم من عدم إدخاله على الفقه القانوني.

أوضحت لجنة حقوق الإنسان التابعة للأمم المتحدة في تعليق عام على المادة 17 أن الحق في الخصوصية يشمل الحق في الحماية «ضد كل تلك التدخلات والاعتداءات سواء أكانت صادرة عن سلطات الدولة أو من الأشخاص الطبيعيين أو الاعتباريين.»[131] ولكن لا يمنح هذا التعليق العام سوى توجيه بسيط عما يعنيه مصطلح "تعسفي" أو "خصوصية". فبخصوص "تعسفي" ذكرت اللجنة أن التدخل المنصوص عليه في القانون يمكن أن يكون تعسفياً، ومن ثم يجب أن تكون كل هذه التدخلات «وفقاً لأحكام وأهداف وأغراض العهد وأن تكون معقولة في أي حال، وفي ظروف محددة».[132] وهذا يقدم في نهاية المطاف توجيه بسيط جداً عما قد يمكن اعتباره «تعسفي»، رغم استبعاد التدخلات في الخصوصية التي تنص عليها القوانين والتي تتعارض مع أغراض العهد أو التي لم تكن معقولة.

ويشتمل التعليق العام كذلك على تصريحات موسعة جداً، وإن كانت عامة، بشأن حماية البيانات، حيث ذكر بأن جمع وحفظ المعلومات الشخصية، سواء من قبل هيئات عامة أو خاصة، لابد أن يخضع لتنظيمات، وأن للأفراد الحق في التأكد من المعلومات التي يُحتفظ بها عنهم وأغراض حفظها والجهة التي تحفظ لديها.[133]

وجاء رأي اللجنة في هذا النطاق أيضاً فضفاض. ففي قضية هولست ضد هولندا (Hulst v. the Netherlands)، كان على اللجنة أن تقيم ما إذا كان اعتراض المكالمات الهاتفية التي كان يجريها المؤلف، والذي

---

131 التعليق العام رقم. 16: الحق في احترام الخصوصية، والأسرة والمسكن والمراسلات وحماية الشرف والسمعة. (المادة 17)، اعتمد بتاريخ 4 أغسطس/ آب 1988، الفقرة: 1.

132 المرجع السابق، الفقرة 4.

133 المرجع السابق، الفقرة 10.

كان محامياً، والتي استخدمت لإدانته بجريمة، كانت تمثل تعدياً غير مبرر على خصوصيته. وفي تقريرها لعدم وجود أي تدخل، استندت اللجنة إلى المعايير المشار إليها أعلاه في تعليقها العام، ورأت أن التدخل كان مصرح به بموجب القانون وكان معقولاً.(134)

2.1.1.3. نظام الدول الإفريقية والبلدان الأمريكية

ليس هناك من حماية صريحة للخصوصية في الميثاق الأفريقي لحقوق الإنسان وحقوق الشعوب.(135) وتوجد أيضاً تدابير حماية الخصوصية ضمن أحكام الاتفاقية الأمريكية لحقوق الإنسان (ACHR)(136) في المادة 11، والاتفاقية الأوروبية لحقوق الإنسان (ECHR)،(137) في المادة 8.

حيث نصت الاتفاقية الأمريكية لحقوق الإنسان على:

(2) لا يجوز أن يتعرض أحد لتدخل اعتباطي أو تعسفي في حياته الخاصة أو في شؤون أسرته أو منزله أو مراسلاته، ولا أن يتعرض لاعتداءات غير مشروعة على شرفه أو سمعته.

(3) لكل إنسان الحق في أن يحميه القانون من مثل ذلك التدخل أو تلك الاعتداءات.

هذه الأحكام هي مشابهة تماماً لتلك التي نص عليها الإعلان العالمي لحقوق الإنسان والعهد الدولي للحقوق المدنية والسياسية. ولم يلق هذا الأمر نظراً قضائياً كبيراً بصورة مباشرة لدى محكمة البلدان الأمريكية لحقوق الإنسان. ففي قضية مهمة أخيرة تتعلق بالخصوصية، في نوفمبر/ تشرين الثاني 2011، وهي فونتيفيكشيا آند داميكو ضد الأرجنتين (Fontevecchia & D'Amico v. Argentina)(138) قررت محكمة البلدان الأمريكية بأن نشر معلومات خاصة عن منعم (Menem)، الرئيس السابق للأرجنتين، لم يكن بمثابة اعتداء على خصوصيته، واستندت في ذلك إلى أن المعلومات كانت معروفة بالفعل، ولم يعتبرها الرئيس منعم (Menem) نفسه على أنها معلومات سرية ولقيت المعلومات اهتماماً كبيرا لدى العامة.

وتناولت محكمة البلدان الأمريكية مسألة الخصوصية في عدد من القضايا الأخرى، منها تريستان دونوسو ضد باناما (Tristán Donoso v. Panama)، تبين للمحكمة وجود انتهاك للحق في الخصوصية عندما نشر مسؤولون بالدولة تسجيلاً لمحادثة هاتفية خاصة، كان قد سجله طرف خاص، إلى مسؤولين في الكنيسة وأعضاء نقابة المحامين.(139) وفي قضية ايشر وآخرون ضد البرازيل (Escher et al. v. Brazil)، توصلت المحكمة إلى عدد من الاستنتاجات المهمة فيما يتعلق بالخصوصية في سياق مراقبة الهاتف؛ الأول، قررت المحكمة أنه حيث يقع عبء إثبات وقائع انتهاك حقوق الإنسان في العادة على كاهل المدعي، فكان من البديهي أن تنتهي المحكمة إلى عجز المدعي عن إثبات هذه الوقائع إثباتاً قطيعاً، وذلك بسبب السرية من جانب الدولة.(140)

---

134 المراسلة رقم. 903/1999، 1 نوفمبر/ تشرين الثاني 2004.

135 أعتمد في 26 يونيو 1981، مستند منظمة الوحدة الأفريقية رقم CAB/LEG/67/3، النسخة 5, 21 I.L.M. 58 (1982)، دخل حيز النفاذ في 21 أكتوبر/ تشرين الأول 1986.

136 اعتمدت في 22 نوفمبر/ تشرين الثاني 1969، سلسلة معاهدات منظمة الدول الأمريكية رقم: 36، دخلت حيز النفاذ في 18 يوليو 1978.

137 اعتمدت في 4 نوفمبر/ تشرين الثاني 1950، E.T.S. رقم: 5، دخلت حيز النفاذ في 3 سبتمبر/ أيلول 1953.

138 29 نوفمبر/ تشرين الثاني 2011، السلسلة ج، رقم 193، الفقرة 83.

139 27 يناير/ كانون الثاني 2009، السلسلة ج، رقم: 193، الفقرة 83.

140 6 يوليو 2009، السلسلة ج. رقم 200، الفقرات 127–128.

ونظراً للطبيعة التدخلية التي تنطوي عليها عملية التنصت على المكالمات الهاتفية، قررت المحكمة ما يلي:

> يتعين أن يستند هذا التدبير على قانون يتميز بالدقة وينص على قواعد واضحة ومفصلة تنظم المراسلات، مثل ملابسات اللجوء إلى هذا التدبير، ومن له الحق في طلب تنفيذه ومن له الصلاحية في أن يأمر به ومن عليه المسؤولية لمباشرته والإجراء المتبع فيه.[141]

في هذه القضية، لم تتبع القواعد على النحو الملائم، ومن ثم لم تستوفى شروط المشروعية في التدخل في الخصوصية، كما هو منصوص عليه في الاتفاقية الأمريكية لحقوق الإنسان.[142] وكان نشر بعض المعلومات السرية من جانب وكلاء الدولة بمثابة تعدياً إضافياً على الحق في الخصوصية.[143]

فيما يتعلق بحماية البيانات، أوضحت لجنة البلدان الأمريكية أنها ترى أن حق الحصول على البيانات (habeas data) منصوص عليه في الاتفاقية الأمريكية لحقوق الإنسان، والذي يعطي الأفراد الحق في معرفة المعلومات التي تحتفظ بها الجهات الحكومية والخاصة به والإطلاع عليها وتعديلها أو تصحيحها أو مسحها، حسب الاقتضاء.[144] ولم يسبق لمحكمة البلدان الأمريكية تناول مسألة أمر الحصول على البيانات (habeas data) بشكل مباشر على الإطلاق.

3.1.1.3. الاتفاقية الأوروبية لحقوق الإنسان: لمحة عامة

صاغت المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان هذا الحق بشروط تختلف عن تلك الواردة في العهد الدولي للحقوق المدنية والسياسية والإعلان العالمي لحقوق الإنسان، على النحو التالي:

(1) لكل إنسان حق احترام حياته الخاصة والعائلية ومسكنه ومراسلاته.

(2) لا يجوز للسلطة العامة أن تتعرض لممارسة هذا الحق إلا وفقاً للقانون وبما تمليه الضرورة في مجتمع ديمقراطي لصالح الأمن القومي وسلامة الجمهور أو الرخاء الاقتصادي للمجتمع، أو حفظ النظام ومنع الجريمة، أو حماية الصحة العامة والآداب، أو حماية حقوق الآخرين وحرياتهم.

إن تكييف الحق في هذه المادة أكثر إيجابية؛ إذ يعتبر حقاً في احترام خصوصية المرء وليس حق يستوجب الحماية من التدخلات. وثمة فرق آخر وهو اقتصار الحماية من التدخل من جانب السلطات العامة، على الرغم من أن المحكمة الأوروبية لحقوق الإنسان لم تفسر الحكم بهذه الطريقة المحدودة (أنظر أدناه). وأخيراً، نجد أن معايير القيود موضوعة في صورة أكثر وضوحاً، فبدلاً من المصطلحات الغامضة مثل "الاعتباطي" و«غير القانوني» و «التعسفي»، يوجد معيار مكون من ثلاثة أجزاء واضحة: أ) وفقاً للقانون؛ ب) الضرورة في مجتمع ديمقراطي، ج) وحماية واحدة من المصالح المذكورة (الأمن القومي وحفظ النظام وهلم جرا).

وفيما يتعلق بنطاق مفهوم الخصوصية، حددت المحكمة الأوروبية عدداً من الأنواع المعينة للإجراءات التي تتخذها الدولة وقد تنتهك الحق، ومنها اعتراض الاتصالات الخاصة أو التنصت على المكالمات الهاتفية، بغض النظر عن فحوى الاتصالات،[145] وتخصيص الحقوق المعنية بالأطفال،[146] والتدخل في الحياة

---

141 المرجع السابق، الفقرة 131.

142 المرجع السابق. الفقرة 146.

143 المرجع السابق. الفقرة 164.

144 لجنة البلدان الأمريكية لحقوق الإنسان، تقرير بشأن وضع مناصري حقوق الإنسان في البلدان الأمريكية، الفقرة 89. متوفر على: http://www.cidh.org/countryrep/defenders/defenderschap1-4.htm

145 أنظر على سبيل المثال لورداشي وآخرون ضد مولدوفا (Iordachi And Others v. Moldova)، 10 فبراير 2009، العريضة رقم: 25198/02. أنظر أيضاً هالفرود ضد المملكة المتحدة (Halford v. the United Kingdom)، 25 يونيو 1997، العريضة رقم:. 20605/92، الفقرة 44.

146 أنظر على سبيل المثال الشولز ضد ألمانيا (Elsholz v. Germany)، 13 يوليو 2000، العريضة رقم: 25735/94

الجنسية،[147] والعلاج الطبي الإلزامي،[148] والحصول على أنواع معينة من المعلومات المملوكة لدى الدولة.[149] وامتنعت المحكمة عن اقتراح تعريف عام للخصوصية بحجة عدم إمكانية ذلك، كما ذكر أعلاه.[150]

ولكن أشارت المحكمة إلى عدد من السمات التي تميز هذا الحق. ففي قضية فون هانوفر ضد ألمانيا (Von Hannover v. Germany)، على سبيل المثال، قررت المحكمة أن الخصوصية تغطي «الجوانب المتعلقة بالهوية الشخصية، مثل اسم الشخص، أو صورة له» و «سلامة الشخص البدنية والنفسية». وعلاوة على ذلك، إن المقصود من الحق هو «ضمان تطور شخصية كل فرد في علاقاته مع غيره من البشر، دون تدخل خارجي.»[151] وفي قضية نيميتز ضد ألمانيا (Niemietz v. Germany) قررت المحكمة "أنه سيكون من المقيد جداً حصر المفهوم ضمن «دائرة داخلية» قد يعيش فيها الفرد حياته الشخصية كما يريد ويستبعد العالم الخارجي منها تماماً». وبدلاً من ذلك، «يجب أن تشمل الحياة الخاصة أيضاً إلى حد ما في ذلك الحق في إنشاء وتطوير العلاقات مع الأشخاص الآخرين.»[152] ودخل ضمن نطاق هذا المفهوم علاقات الأعمال والعلاقات المهنية، فاعتبر البحث عن مراكز الأعمال تدخلاً في الحياة الخاصة.[153]

وقد أشارت المحكمة إلى أن «توقعات الشخص المعقولة بشأن الخصوصية قد تكون عاملاً مهماً، وإن لم يكن قاطعاً بالضرورة».[154] حتى إن المعلومات التي تم جمعها في الحالات العامة قد تثير مسائل تتعلق بالحياة الخاصة من خلال الاستخدام غير المتوقع الذي تتعرض له. ومن ثم: "قد تنشأ اعتبارات الحياة الخاصة – على الرغم من ذلك – بمجرد ظهور سجل منهجي أو دائم عن هذه المواد من النطاق العام."[155]

في الواقع، اتجهت المحكمة إلى الاعتراف بنطاق واسع إلى حد ما من الحق، مع الاعتراف أيضاً بإمكانية فرض القيود، بالإضافة إلى هامش واسع من التقدير للدول، وخصوصاً في القضايا التي تنطوي على حماية الأطفال. فعلى سبيل المثال، في قضية كيغان ضد أيرلندا (Keegan v. Ireland)، ذكرت المحكمة أن الدول «تتمتع بهامش واسع من التقدير فيما يتعلق بالتبني». [156] حيث تضمنت القضية أب يسعى إلى الحصول على وصاية على طفل له قامت أم الطفل، التي نفرها الأب، بالتقدم لتبني هذا الطفل. وفي قضية فون هانوفر ضد ألمانيا (Von Hannover v. Germany) (رقم 2)، التي تضمنت نشر صور يدعى أنها خاصة، قالت المحكمة:

---

147 أنظر على سبيل المثال دودجيون ضد المملكة المتحدة (Dudgeon v. the United Kingdom) (22 أكتوبر/ تشرين الأول 1981، العريضة رقم: 7525/76، أنظر أيضاً موسلي ضد المملكة المتحدة (Mosley v. The United Kingdom)، 10 مايو2011، العريضة رقم: 48009/08.

148 أنظر على سبيل المثال أكماني وآخرون ضد بلجيكا (Acmanne and others v. Belgium) (10 ديسمبر/ كانون الأول 1984، قرار قبول الدعوى، العريضة رقم: 10435/83.

149 أنظر على سبيل المثال غاسكين ضد المملكة المتحدة (Gaskin v. United Kingdom)، الحاشية 167.

150 أنظر نيميتز ضد ألمانيا (Niemietz v. Germany) في الحاشية 127. في قضية كاستيلو-روبيرتس ضد المملكة المتحدة (Costello-Roberts v. the United Kingdom)، قررت المحكمة أن مبدأ الحياة الخاصة "لا يمكن تعريفه تعريفاً جامعاً". 25 مارس/ آذار1993، العريضة رقم: 13134/87، الفقرة 36. اشتملت القضية على عقاب بدني في مدرسة خاصة والتي قررت المحكمة في حيثياتها أنها لا تمثل تعدياً على الحياة الخاصة.

151 24 يونيو 2004، العريضة رقم: 59320/00، الفقرة 50. تم مسح الإشارة المرجعية إلى القضايا والنصوص القانونية الأخرى هنا وكذلك من الاقتباسات الأخرى في النص.

152 16 أكتوبر/ تشرين الأول 1992، العريضة رقم: 13710/88، الفقرة 29.

153 أنظر أيضاً فون هانوفر ضد ألمانيا (Von Hannover v. Germany) (رقم 2) 7 فبراير 2012، العريضة رقم: 40660/08، والعريضة رقم: 60641/08، الفقرة 95.

154 بي جي آند جي إتش ضد المملكة المتحدة (P.G. AND J.H. v. United Kingdom)، 25 سبتمبر/ أيلول 2001، العريضة رقم: 44787/98 الفقرة 57.

155 أنظر أيضاً فون هانوفر ضد ألمانيا (Von Hannover v. Germany) (رقم 2) 7 فبراير 2012، العريضة رقم: 40660/08، والعريضة رقم: 60641/08، الفقرة 95.

156 26 مايو 1994، العريضة رقم: 16969/90، الفقرة 47.

«للدول المتعاقدة هامش محدد من التقدير في تقييم حالات ومدى ضرورة التدخل في حرية التعبير التي يكفلها هذا الحكم».[157]

4.1.1.3. الاتفاقية الأوروبية لحقوق الإنسان: القيود

لقد وضعت المحكمة منهجية واضحة إلى حد ما لتطبيق الاختبار الثلاثي للقيود على القضايا التي تنطوي على التدخل في الخصوصية. وفي عدد من القضايا، وخاصة فيما يتعلق بالتنصت على المكالمات الهاتفية وغيرها من أشكال المراقبة، أشارت المحكمة إلى أنه نظراً لطبيعة هذه الأنشطة التي تتميز بالتعدي على الخصوصية بشكل خاص، يجب "أن تقوم على أساس" القانون « الذي يتميز بالدقة في الأساس ... خاصة في ظل استمرار تقدم التكنولوجيا المتوفرة للاستخدام.»[158] وفي قضية كروسلين ضد فرنسا (Kruslin v. France)، قضت المحكمة أن هذا الجزء من الاختبار لم يستوفِ بسبب غياب الدقة الكافية في شروط التنصت على المكالمات الهاتفية. وعلى وجه الخصوص، لم تكن هناك قيود على فئات الأشخاص الذين يمكن التنصت على هواتفهم، أو التزام على القضاة بتحديد حد زمني للتنصت، أو إجراءات إعداد تقارير بالمحادثات التي تم اعتراضها أو إجراءات إتلاف التسجيلات، ولم يمكن هناك ما يتطلب حفظ التسجيلات سليمة دون المساس بها.[159]

في قضية مالون ضد المملكة المتحدة (Malone v. United Kingdom)، بحثت المحكمة الأوروبية في ممارسة "قياس" المكالمات الهاتفية (أي تسجيل أرقام ومدة المكالمات). وميزت المحكمة بين هذه الممارسة وبين الاعتراض الفعلي للمكالمات، ولكنها أشارت إلى أنه على الرغم من مشروعية هذه الممارسة (على افتراض أنها قائمة على أساس الموافقة) لأغراض إعداد الفواتير ومراقبة الاستخدام السليم للخدمة، إلا أن تمرير هذه المعلومات إلى الشرطة كان يمثل تدخلاً في الحياة الخاصة. ولم يكن هناك أي قانون يطلب من مكتب البريد، الذي كان يجري عملية القياس (وهي هيئة عامة تحولت إلى المؤسسة البريطانية للاتصالات السلكية واللاسلكية (British Telecommunications) عند النظر في القضية)، أن يمرر التسجيلات إلى الشرطة، ولكن قام بذلك في الحالات التي كانت تمثل فيها هذه المعلومات «ضرورة لتحقيقات الشرطة في شأن الجرائم الخطيرة" وكان يتعذر الحصول عليها من مصادر أخرى.» وهذه الممارسة لم تفي بمعيار «التوافق مع القانون» الواردة ضمن المادة 8 (2) من الاتفاقية الأوروبية لحقوق الإنسان.[160] وهذا الأمر متصل بشكل واضح بالحالات الأخرى التي تنخرط فيها الجهات الخاصة – مثل مزودي خدمة الإنترنت – مع الهيئات العامة في ممارسات لها تأثير على حقوق الخصوصية.

فيما يتعلق بالجزء الثاني من الاختبار، بشكل عام، لم تجد المحكمة ما يمنعها في أن تقر الغاية المشروعة التي تستوجب الحماية في قضايا الخصوصية، والتي دائماً ما تتصل بحقوق الآخرين وحفظ النظام. ومن ثم، قررت المحكمة في قضية ليندر ضد السويد (Leander v. Sweden) في فقرة موجزة بأن القانون الذي يسمح للشرطة بالحفاظ على سرية المعلومات التي جمعت عن المتقدمين لشغل مناصب معينة كان ضرورياً من أجل مصلحة الأمن القومي،[161] أما في قضية موراي ضد المملكة المتحدة (Murray v. the United Kingdom) أشارت المحكمة أيضاً إلى فقرة واحدة فقط للإقرار بأن منع وقوع الجريمة هو من الأغراض المشروعة.[162]

---

157 الحاشية 153، الفقرة 104.

158 أنظر على سبيل المثال كروسلين ضد فرنسا (ecnarF .v nilsurK)، 42 إبريل 0991، العريضة رقم: 10811/58، الفقرة 33. أنظر أيضاً روتارو ضد رومانيا، الحاشية 155، الفقرة 62، والتي تشتمل على جمع البيانات الشخصية.

159 المرجع السابق، كروسلين ضد فرنسا (Kruslin v. France)، الفقرة 35.

160 مالون ضد المملكة المتحدة (Malone v. United Kingdom)، 2 أغسطس/ آب 1984، العريضة رقم: 8691/79 الفقرة 83 إلى 86.

161 26 مارس/ آذار1987، العريضة رقم: 9248/81. الفقرة 49.

162 28 أكتوبر/ تشرين الأول 1994، العريضة رقم: 14310/88، الفقرة 89.

ولتقييم ضرورة كل جزء من أجزاء الاختبار، ذكرت المحكمة: «إنه لا بد من الأخذ بعين الاعتبار التوازن الكافي الذي يجب إيجاده بين المصالح المتقابلة لكل من الفرد والمجتمع ككل».[163] وعلاوة على ذلك، «ينطوي مفهوم الضرورة على أن يلبي التدخل حاجه اجتماعية ملحة ويتناسب على وجه الخصوص مع الهدف المشروع المقصود منه» وأن «تكون الأسباب التي يستند إليها لتبرير التدخلات في القضية «أسباب ذات صلة وكافية».[164] وفيما يتعلق بالمحاكم الوطنية، استندت المحكمة الأوروبية على فكرة المصلحة العامة العليا في تقييم القيود على الخصوصية، وخصوصاً عندما يتعلق الأمر بحقوق الإنسان، كما هو واضح في المربع أدناه من قضية هانوفر فون (Von Hannover).

5.1.1.3. الاتفاقية الأوروبية لحقوق الإنسان: الجهات الخاصة

تناولت المحكمة الأوروبية مسألة التدخل في الخصوصية على أساس مصالح خاصة في عدد من القضايا. وأكدت أن «الغرض من [المادة 8] هو «أساساً» حماية الفرد من التدخل التعسفي من قبل السلطات العامة».[165] وقد أقرت المحكمة بأن المصالح الخاصة قد تفرض التزامات إيجابية على الدول بأن تتخذ ما يلزم من إجراءات لحماية الخصوصية. وفي بعض الأحيان، تستخدم المحكمة التزامات إيجابية في المسائل التي «لا تكون الدولة هي من اتخذ التدابير، ولكن تكون قد أخفقت في اتخاذ تدابير» لحماية الخصوصية.[166] وتتعلق بعض هذه القضايا بالعلاقة بين الأفراد والدولة، أو التطبيق «العمودي» للحقوق، ومن الأمثلة على ذلك قضية غاسكين ضد المملكة المتحدة (Gaskin v. United Kingdom)، والتي قضت فيها المحكمة أن الهيئة العامة ألزمت بنشر بعض المعلومات الشخصية المتعلقة بمقدم الطلب لحماية الخصوصية.[167]

في الوقت نفسه، أشارت المحكمة في بعض الحالات إلى الالتزامات الإيجابية على الدول في تنظيم العلاقات بين الجهات الفاعلة من غير الدول، وهو ما يعرف بالتطبيق «الأفقي» للحقوق. وفي مثل هذه الحالات، لا يتعلق الأمر بالعلاقة بين الدولة والفرد – إما بسبب إجراء اتخذته الدولة أو بسبب إخفاقها في اتخاذ إجراء ما. بل إن الأمر يكمن في أن الحماية الفعالة للحياة الخاصة تقتضي من الدولة تنظيم العلاقات بين الجهات الفاعلة من غير الدول، مثلاً من خلال توفير سبل الإنصاف القانونية ضد حملات التعدي على الخصوصية.

ونجد في بعض هذه القضايا عنصر مشاركة الدولة في انتهاك الخصوصية. فعلى سبيل المثال، في قضية لوبيز أوسترا ضد إسبانيا (López Ostra v. Spain)، قررت المحكمة أن تقاعس السلطات عن اتخاذ ما يلزم من إجراءات لمنع الآثار الضارة المترتبة على التلوث البيئي الشديد الناشئ عن محطة معالجة النفايات يعد خرقاً لأحكام المادة 8. ولكن أشارت المحكمة على وجه التحديد إلى أن شرعية المصنع بموجب القانون الإسباني كان

---

163 كيغان ضد أيرلندا (Keegan v. Ireland)، الحاشية 156، الفقرة 49.

164 أولسون ضد السويد، 24 مارس/ آذار1988، العريضة رقم: 10465/83، الفقرة 67 و 68.

165 أنظر ماركس ضد بلجيكا (Marckx v. Belgium)، 13 يونيو 1979، العريضة رقم: 6833/74، الفقرة 31.

166 إيري ضد أيرلندا (Airey v. Ireland)، 9 أكتوبر/ تشرين الأول 1979، العريضة رقم: 6289/73، الفقرة 37.

167 غاسكين ضد المملكة المتحدة (Gaskin v. United Kingdom)، 7 يوليو 1989، العريضة رقم: 10454/83، الفقرة 41 و 49.

محط تساؤلات وركزت على حقيقة أن السلطات لم تخفق في حماية السيدة لوبيز أوسترا (López Ostra) فحسب، بل شاركت أيضاً في إطالة أمد الوضع القائم.[168] وفي قضية إكس و واي في ضد هولندا (X and Y v. the Netherlands)،[169] رأت المحكمة أن الإجراءات المدنية لم تكن كافية لحماية الأفراد من الاعتداء الجنسي، وأنه يتعين وضع تدابير جنائية في هذا الشأن. تقدمت هولندا بقانون جنائي يتعلق بالاعتداء الجنسي؛ ولكن لم ينطبق على هذه القضية بسبب بعض المسائل الإجرائية المتعلقة بإعاقة المجني عليها ذهنياً.

ولكن في قضايا أخرى رأت المحكمة أن الدول كانت تخترق الحق في الخصوصية لمجرد الإجراءات التي كانت بين الأطراف الخاصة (أنظر المربع).

12) قضيتا فون هانوفر ضد ألمانيا (Von Hannover v. Germany)

أصدرت المحكمة الأوروبية لحقوق الإنسان قرارين الأول في عام 2004 والثاني في عام 2012 في قضية فون هانوفر ضد ألمانيا (Von Hannover v. Germany) وقضية هانوفر فون ضد ألمانيا الثانية (Von Hannover v. Germany)، نصت فيهما على قواعد واضحة بشأن الخصوصية. فاشتملت القضية الأولى على عدد من الصور للأميرة كارولين (Princess Caroline) في موناكو تضمن صوراً لها وهي تمتطي الخيل، وأثناء قضائها لعطلة التزلج، وأخرى أثناء تعثرها بشيء على شاطئ خاص. نشرت الصور في مجلات خاصة في ألمانيا، ومن ثم تعلقت القضية بالتطبيق الأفقي للحقوق. أيدت المحاكم الألمانية نشر أي صور بشكل عام (باستثناء بعض الصور التي أخذت في أماكن حظيت الأميرة بوجود خصوصية مناسبة فيها وبعض الصور التي ظهر فيها أطفالها).

لم يختلف الوضع كثيراً في القضية الثانية، باستثناء أن الصور المذكورة ركزت في معظمها على مسألة مرض الأمير الحاكم لموناكو، الأمير رينييه (Prince Rainier)، وطريقة رعاية أسرته له خلال مرضه.

في القضية الأولى ذكرت المحكمة الأوروبية ما يلي:

> في المسائل التي تستوجب على المحكمة إيجاد توازن بين حماية الحياة الخاصة وحرية التعبير، تم التأكيد دوماً على مدى إسهام الصور أو المقالات التي تنشرها الصحافة في المصلحة العامة.[170]

وذكرت المحكمة ما يلي:

> ترى المحكمة أنه يتعين وضع تفرقة أساسية بين الإبلاغ عن الوقائع – حتى تلك المثيرة للجدل – التي من شأنها أن تحدث جدلاً في مجتمع ديمقراطي يتعلق بالسياسيين في إطار ممارستهم لمهامهم مثلاً، وبين الإبلاغ عن تفاصيل حياة خاصة لفرد لا يمارس مهاماً رسمية في هذه القضية. [171]

وذكرت المحاكم المحلية بأن الأميرة كارولين كانت شخصية من شخصيات مجتمع معاصر «بامتياز»، ومن ثم لم يكن لديها أي حق في الخصوصية ما لم تكن في مكان منعزل عن أعين الجمهور. ورأت المحكمة الأوروبية أن هذا المعيار قد يكون مناسباً لممارسة المهام الرسمية للسياسيين، ولكن لا ينطبق في هذه الحالة. كما لاحظت المحكمة فيما يتعلق بالمدعي بأن «مصلحة الجمهور العام والصحافة مستمدة فقط من انتمائها إلى العائلة المالكة نفسها وإن لم تمارس أية مهام رسمية.»[172]

---

168 9 ديسمبر/ كانون الأول 1994، العريضة رقم: 16798/90، الفقرة 54 إلى 56.

169 26 مارس/ آذار1985، العريضة رقم: 8978/80.

170 الحاشية 151، الفقرة 60.

171 المرجع السابق، الفقرة 63.

172 المرجع السابق، الفقرة 72.

- في القضية الثانية، وضعت المحكمة عدداً من المبادئ التي ينبغي أخذها في الاعتبار عند موازنة حرية التعبير مع حماية الخصوصية، وكان من بين هذه المبادئ:
- إلى أي مدى ساهم المنشور في مسألة تتعلق بالمصلحة العامة (الفقرة 109)؛
- درجة شهرة الشخص المعني وموضوع التقرير (الفقرة 110)؛
- السلوك السابق للأشخاص المعنيين (الفقرة 111)؛
- مضمون وشكل وعواقب المنشور (الفقرة 112)،
- والظروف التي تم فيها التقاط الصور (الفقرة 113).

بشكل عام، يبدو أن المحكمة كانت على استعداد لأن تسمح بحرية واسعة، حتى في الصور، الأمر الذي أسهم في الجدل الدائر بشأن مسألة من مسائل المصلحة العامة. وهنا نجد أن غياب هذه المساهمة في القضية الأولى – ربما أفضل مثال على ذلك تصوير الأميرة كارولين (Princess Caroline) عندما تعثرت على الشاطئ – استوجب نتيجة محددة، بينما في القضية الثانية رأت المحكمة أن «المقالات التي نشرت حول مرض الأمير رينييه الثالث (Prince Rainier III)، والذي يمثل السيادة الحاكمة لإمارة موناكو في ذلك الوقت، وسلوك أفراد عائلته خلال فترة مرضه» هي مسألة تتصل بالمصلحة العامة.[173]

6.1.1.3. الاتفاقية الأوروبية لحقوق الإنسان: حماية البيانات

لم يسبق للمحكمة أن تقر أي حق عام في حماية البيانات بموجب المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان، على الأقل في إطار استعمال هذا المصطلح. ومع ذلك، أقرت في سلسلة من القضايا جوانب متعددة للحقوق المسلم بها عموماً والمرتبطة بحماية البيانات.

أولاً، قررت المحكمة في عدد من أحكامها بأن جمع المعلومات الشخصية ينطوي على قلق بشأن الحياة الخاصة؛ ومن ذلك على سبيل المثال قضية موراي ضد المملكة المتحدة (Murray v. the United Kingdom)، التي لم تعترض فيها الحكومة، وقبلت المحكمة بأن جمع المعلومات الشخصية (بما في ذلك الصور) عند القبض على أي شخص يشكل تدخلاً في الحياة الخاصة، رغم أن ذلك تم تبريره باعتباره قيد على هذا الحق في ملابسات هذه القضية.[174]

وفي قضية ليندر ضد والسويد (Leander v. Sweden) رأت المحكمة أن تخزين المعلومات المتعلقة بالحياة الخاصة ونشرها يمثلان تدخلاً في الخصوصية.[175] وناقشت المحكمة في هذه القضية بشيء من التفصيل الضمانات الإجرائية التي كانت ضرورية لضمان توافق عملية جمع المعلومات – في هذه القضية المعنية بمدى ملائمة الشخص للعمل في متحف بحري – مع شرط الضرورة في مجتمع ديمقراطي. وقبلت المحكمة أن جمع هذا النوع من المعلومات قد يكون ضرورياً في حماية الأمن القومي. إلا أنها استوجبت توافر «ضمانات مناسبة وفعالة ضد أية انتهاكات.»[176] وأشارت إلى أن القانون المتصل بذلك اشتمل على أحكام تقيد استعمال المعلومات إلى أدنى حد ممكن، وخاصة خارج نطاق المسائل التي تخضع لسيطرة المسؤولين، حيث يمكن استخدامها فقط لأغراض الملاحقة القضائية والحصول على الجنسية. وركزت المحكمة بشكل خاص على دور الفاعلين الخارجيين في ممارسة الرقابة على النظام، بما في ذلك أعضاء البرلمان ووزير العدل وأمين المظالم بالبرلمان واللجنة البرلمانية المعنية بالعدل.

---

173 الحاشية 153، الفقرة 117.

174 الحاشية 162، الفقرة 86.

175 الحاشية 161. أنظر أيضاً روتارو ضد رومانيا (Rotaru v. Romania)، الحاشية 158.

176 المرجع السابق، الفقرة 60.

ثانياً، رأت المحكمة أن نشر المعلومات الشخصية من جانب الجهات العامة ينطوي على مخاوف تتعلق بالخصوصية؛ ففي قضية زد ضد فنلندا (Z. v. Finland) تعلق الأمر بالكشف عن معلومات معينة عن المدعي، منها إصابته بفيروس نقص المناعة البشرية (HIV) خلال سير الإجراءات القضائية. ولم تجد المحكمة ما يعيقها في أن تقرر بأن ذلك كان تدخلاً في حق المدعي في الحياة الخاصة. ورأت المحكمة أن حماية هذه البيانات الشخصية، وبالأخص السجلات الطبية، هو أمر «له أهمية أساسية في تمتع الشخص بحقه في احترام الحياة الخاصة والحياة العائلية.»[177] ونظراً للطبيعة الحساسة التي تنطوي عليها المعلومات الطبية المعنية، "فإن أي إجراءات من جانب الدولة من شأنها أن تلزم بنشر هذه المعلومات أو الكشف عنها دون موافقة المريض تتطلب من المحكمة أن توليها أقصى عنايتها بشأن الضمانات المخصصة لتأمين الحماية الفعالة لها."[178] وركزت المحكمة في معرض تأييدها للكشف عن أدلة معينة على أساس محدود، على شرط إعطاء المدعي الفرص الكافية لرفض الكشف عن بياناته ومدى أهمية المعلومات كأدلة في قضية جنائية خطيرة.[179] ولكن أشارت المحكمة أن الكشف العلني عن المعلومات بعد عشر سنوات فضلًا عن الكشف عنها في حكم محكمة الاستئناف عند توافر خيارات أخرى (مثل عدم ذكر الاسم) كانت بمثابة خرق الحق في الحياة الخاصة.[180]

وحتى الكشف الداخلي (مثل الكشف ضمن القطاع العام) أثار مشاكل تتعلق بالخصوصية. حيث تضمنت قضية إم إس ضد السويد (M.S. v. Sweden) الكشف عن معلومات طبية معينة من جانب عيادة طبية عامة إلى مكتب التأمينات الاجتماعية في سياق طلب مقدم إلى المكتب للحصول على خصائص تتعلق بالحالة المرضية لصاحبة الطلب. ولم يكن من شك بأن الأمر انطوى على مسائل تتعلق بالحياة الخاصة. فرفضت المحكمة ما ادعت به الحكومة من أن صاحبة الطلب بتقديمها للطلب قد وافقت على الكشف عن معلوماتها،[181] وذلك إلى حد ما لأنها لم تحدد. وأشارت المحكمة عند تأكيدها بأن التدخل كان مبرراً لضرورة حصول المكتب على المعلومات حتى يتمكن من تقييم طلب التأمين والضمانات القوية للسرية، مثل فرض عقوبات صارمة في حال الكشف عن المعلومات خارج نطاق دقيق للقانون.[182]

ثالثاً، في عدد من القضايا – بما في ذلك قضية ليندر ضد السويد (Leander v. Sweden)،[183] وقضية غاسكين ضد المملكة المتحدة (Gaskin v. United Kingdom)،[184] وقضية جويرا و أورس ضد إيطاليا (Guerra and Ors. v. Italy)،[185] وقضية جينلي وإغان ضد المملكة المتحدة (McGinley and Egan v. United Kingdom)،[186] وقضية أوديفر ضد فرنسا (Odièvre v. France)،[187] وقضية روتشي ضد المملكة المتحدة (Roche v. United Kingdom)[188] – أيدت المحكمة حق الفرد في الإطلاع على المعلومات الموجودة بحوزة السلطات العامة والمتعلقة به. وفي كل قضية من هذه القضايا، تبين للمحكمة أن الحرمان من الوصول إلى هذه المعلومات هو تدخل في الحق في الحياة الخاصة و/أو الأسرية، وإن سمحت في بعض القضايا بمشروعية التقييد من هذه الحقوق في عدم السماح للوصول إلى هذه المعلومات.

---

177 25 فبراير 1997، العريضة رقم: 22009/93، الفقرة 94.

178 المرجع السابق، الفقرة 96.

179 المرجع السابق، الفقرات 101–109.

180 المرجع السابق، الفقرات 111–113. أنظر أيضاً روتارو ضد رومانيا (Rotaru v. Romania)، الحاشية 158.

181 22 أغسطس/ آب 1997، العريضة رقم: 20837/92، الفقرة 35

182 المرجع السابق، الفقرتان 42 و43.

183 الحاشية 175.

184 7 يوليو 1989، العريضة رقم: 10454/83، 12 EHRR 36.

185 19 فبراير 1998، العريضة رقم: 14967/89.

186 9 يونيو 1998، العريضة رقم: 21825/93، والعريضة رقم: 23414/94.

187 13 فبراير 2003، العريضة رقم: 42326/98.

188 19 أكتوبر/ تشرين الأول 2005، العريضة رقم: 32555/96.

13) قضايا نظرت فيها المحكمة الأوروبية لحقوق الإنسان بشأن الوصول إلى المعلومات الشخصية

في القضية الأولى بشأن الوصول إلى المعلومات الخاصة أمام المحكمة الأوروبية، ***ليندر*** (Leander)، كان المدعي قد تم فصله من وظيفته لدى الحكومة السويدية لأسباب أمنية وطنية ولكن مُنع من الوصول إلى معلومات عن حياته الخاصة المودعة في سجل سري لدى الشرطة والتي على أساسها تم فصله. رأت المحكمة أن تخزين واستخدام المعلومات إلى جانب رفض منح المدعي فرصة دحض ذلك كان بمثابة تدخل في حقه في احترام الحياة الخاصة. ولكن تم تبرير التدخل على أنه ضروري لحماية الأمن القومي السويدي.[189] ومن المثير أنه اتضح في نهاية المطاف أن فصل ليندر (Leander) من عمله كان بسبب معتقداته السياسية، وقد منحته الحكومة اعتذاراً وتعويضاً عن ذلك.

في قضية ***غاسكين*** (Gaskin) طالب المدعي، الذي كان طفلاً تحت رعاية السلطات المحلية في المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية، بالوصول إلى سجلات القضية المتعلقة به لدى الدولة، ولكنه حُرم من ذلك. ورأت المحكمة أن للمدعي الحق في الحصول على المعلومات اللازمة لمعرفة وفهم طفولته ونموه في وقت مبكر، على الرغم من وجوب توازن ذلك مع مصالح الأطراف الثالثة في السرية والذين ساهموا في المعلومات. ومن الجدير بالأهمية أن هذا الأمر وضع التزاماً إيجابياً على الحكومة لإنشاء هيئة مستقلة لتقرر ما إذا كان ينبغي منح حق الوصول إلى المعلومات في حال عدم وجود الطرف الثالث المساهم أو منع الموافقة على الإفصاح. وبما أن الحكومة لم تفعل ذلك، فقد تعرضت حقوق مقدم الطلب إلى الانتهاك.[190]

أما في قضية ***غويرا*** (Gurra) ادعى المدعون الذين كانوا يقطنون بالقرب من مصنع مواد كيميائية «عالية المخاطر» أن السلطات المحلية في إيطاليا لم تقدم لهم معلومات حول مخاطر التلوث وكيفية التصرف في حالة وقوع حادث كبير. ورأت المحكمة أن المشاكل البيئية الحادة قد تؤثر على رفاه الأفراد وتحرمهم من التمتع بحياتهم في منازلهم، وبالتالي فهي بمثابة تدخل في حقهم في الحياة الخاصة والعائلية. ونتيجة لذلك، تحملت السلطات الإيطالية التزاماً إيجابياً بتزويد المدعين بالمعلومات اللازمة لتقييم المخاطر الناجمة عن العيش في بلدة على مقربة من مصنع مواد كيميائية ذات مخاطر عالية. فكان تقاعس الحكومة عن تزويد المدعين بتلك المعلومات الأساسية بمثابة خرق لما ورد في المادة 8 من حقوق.[191] وكان للقرار أهمية خاصة لأنه أظهر عدم حيازة الدولة للمعلومات المطلوبة، فكان عليها الخروج ومباشرة جمعها.

في قضية ***مجينلي وإجان*** (McGinley and Egan)، تعرض المدعون للإشعاع خلال التجارب النووية في جزر كريسماس، وطالبوا بالاطلاع على السجلات المتعلقة بالمخاطر الصحية المحتملة إثر هذا التعرض. ورأت المحكمة أن للمدعين الحق في الوصول إلى المعلومات المذكورة بموجب المادتين 6 و 8 من الاتفاقية الأوروبية لحقوق الإنسان فيما يتعلق بالحق في محاكمة عادلة واحترام الحياة الخاصة والعائلية على التوالي. ومع ذلك التزمت الحكومة بالتزاماتها الإيجابية من خلال وضع عملية يمكن من خلالها الوصول إلى المعلومات، والتي لم يتمكن المدعون من الاستفادة منا.[192]

في قضية ***أوديفر*** (Odièvre)، كانت المسألة تتمحور حول الحصول على معلومات عن الأم الطبيعية للمدعي. وقبلت المحكمة بأن ما حدث هو تدخل في الحق في الحياة الخاصة المكفول بالمادة 8، ولكن

---

189 ليندر (Leander)، الحاشية 183، الفقرات 48 و 67.

190 غاسكين (Gaskin)، الحاشية 184، الفقرة 49.

191 غويرا (Guerra)، الحاشية 158، الفقرة 60.

192 مجينلي وإجان (McGinley and Egan)، الحاشية 186، الفقرات 102–103.

رأت أن رفض السلطات الفرنسية تقديم المعلومات يمثل توازناً مناسباً بين مصالح المدعي ومصالح والدته التي كانت تسعى صراحة للحفاظ على سرية هويتها.[193]

وفي قضية ***روتشي*** (Roche) التي لم تختلف عن قضية ***مجينلي وإجان*** (McGinley and Egan) في اشتمالها على الادعاء بمشاكل طبية ناتجة عن اختبارات عسكرية، رأت المحكمة أنه قد وقع انتهاكاً للحق في الخصوصية لعدم امتلاك الحكومة لأسباب معقولة لرفضها الكشف عن المعلومات. ومن الجدير بالذكر أن المحكمة رأت أن عمليات الإفصاح المختلفة التي تمت كاستجابة لطلبات المدعي لم تشكل «نوعاً من عملية الكشف المنظمة التي نصت عليها المادة 8».[194]

رابعاً، تطرقت المحكمة في بعض القضايا على الأقل، خاصة قضية روتارو ضد رومانيا (Rotaru v. Romania) إلى الحق في دحض المعلومات التي اتضح زيفها.[195] تضمنت القضية معلومات تحوز عليها الأجهزة الأمنية، وكان من الواضح زيف تلك المعلومات ومنع المدعي حق الوصول إليها أو فرصة تصحيحها.

ويبدو واضحاً من هذه القرارات أن جمع المعلومات الخاصة ونشرها، بما في ذلك داخل القطاع العام، سوف تثير دائماً مخاوف تتصل بالحياة الخاصة. ومن ثم تقوم المحكمة في معرض تقييمها لمدى ضرورة جمع هذه المعلومات ونشرها في مجتمع ديمقراطي بتقييم الاستخدام المخصص للمعلومات. وقد أشارت المحكمة أيضاً إلى الحق في دحض (وربما ضمناً تصحيح) المعلومات التي يعتقد صاحبها أنها غير صحيحة. وأدركت المحكمة على الأقل مدى أهمية هيئات الرقابة المستقلة وقد تستعين بها في البت في المسائل المتصلة بحماية البيانات.

ومع ذلك، عندما يتعلق الأمر بالحصول على المعلومات، والمعلومات الشخصية التي تتعلق بالمدعي، توخت المحكمة الحذر، فرفضت الاعتراف بحق عام في الوصول إلى المعلومات الشخصية للفرد، وحصرت بدلاً من ذلك حق الوصول على القضية المطروحة أمامها. وكانت المحكمة في كل قضية تتولى أولاً تقييم ما إذا كان الوصول إلى المعلومات أمراً ضرورياً لحماية حق المدعي في الخصوصية و/ أو الحياة الأسرية من عدمه. وبعبارة أخرى، كان يُمنح الحق في الوصول إلى المعلومات عند الحاجة لحماية مصالح خصوصية أخرى، ولكن لم يُعترف بحق الوصول نفسه على أنه مصلحة تتصل بالخصوصية. يضاف إلى ذلك أن في كل هذه القضايا كانت المعلومات بحوزة هيئة عامة، ومن غير الواضح أن تقوم المحكمة بتطبيق نفس المنطق، عبر التزام إيجابي على الدولة، لطلب الإفصاح عن المعلومات من الهيئات الخاصة.

كانت هناك بضعة قضايا مطروحة لدى المحكمة الأوروبية لحقوق الإنسان تتصل مباشرة بمسألة الخصوصية والإنترنت. وهذه يوحي بأن الطبيعة المعقدة والمختلفة التي تتميز بها شبكة الإنترنت قد تثير بعض المسائل المعقدة للخصوصية. ومن ثم كانت قضية كي يو ضد فنلندا (K.U. v. Finland) تتصل بما إذا كان يجب إجبار مزود خدمة الإنترنت على الكشف عن هوية شخص استخدم خدماته لنشر إعلان ينتحل فيه شخصية فرد آخر، وهو صبي يبلغ من العمر 12 عاما، حيث قام «بانتحال» صورة الصبي وادعى أنه كان يبحث عن «علاقة حميمة مع صبي من عمره أو أكبر منه سناً» ليرشده إلى الطريق الصواب».[196] رفض مزود خدمة الإنترنت الطلب، وأيدت ذلك المحاكم المحلية لأن القانون الفنلندي ينص على أنه لا يجوز إلا للشرطة أن تكشف عن هذه المعلومات في حالات محددة لا تدخل ضمنها هذه الحالة، والتي كانت واحدة من حالات التحريف المغرض.

---

193 أوديفر (Odièvre)، الحاشية 187، الفقرات 44–49.

194 روتشي (Roche)، الحاشية 188، الفقرة 166.

195 الحاشية 158، الفقرة 46.

196 2 ديسمبر/ كانون الأول 2008، العريضة رقم: 2872/02، الفقرة 7.

اطلعت المحكمة الأوروبية خلال نظرها في القضية على مجموعة واسعة من الصلاحيات الدولية من مجلس أوروبا ومنظمة الأمم المتحدة والاتحاد الأوروبي. فتيسر لها أن تقرر بأن القضية تتعلق بالحياة الخاصة، "وهو مفهوم يغطي السلامة الجسدية والمعنوية للشخص."[197] وأشارت المحكمة أن على الدول التزام إيجابي بموجب المادة 8 لتجريم الاعتداء على الشخص، وبخاصة عندما يبلغ الأمر الاعتداء على الأطفال وسائر الضعفاء من أفراد، ولكن لن يكون لهذا التجريم أثر رادع ما لم يتم الكشف عن الجاني. ولم يتوقف الأمر عند حد المطالبة بالتعويض عن الأضرار ضد مزود خدمة الإنترنت، لأن ما يمثل بالضرورة التأثير الرادع هو ملاحقة الجاني الحقيقي بشكل مباشر.

وأشارت المحكمة إلى الحاجة إلى الحماية الكافية لقرينة البراءة وأن «حرية التعبير وسرية الاتصالات هي اعتبارات أساسية ولابد من حصول مستخدمي خدمات الاتصالات والإنترنت على ضمان باحترام خصوصياتهم وحرية تعبيرهم». ولكن بمجرد استبعاد الكشف عن المعلومات، لم تطبق الدولة أي «إطار للتوفيق بين مختلف المطالبات التي تتنافس من أجل الحماية في هذا السياق»، ومن ثم كانت مخالفة للالتزامات المنصوص عليها في المادة 8.[198] فأدركت المحكمة ذلك التوازن المعقد الذي يتعين إيجاده بين الحقوق للبت في هذه القضية، ولكنها لم تباشر وضع هذا التوازن بنفسها.

2.1.3. حماية البيانات

1.2.1.3. المعايير العالمية

تتصل الأنظمة المعنية بحماية البيانات اتصالات مباشرا بحماية الخصوصية على شبكة الإنترنت، نظراً لأنها صُممت خصيصاً لمعالجة ما يتعلق بجمع البيانات والخصوصية من مسائل ناتجة عن التقنيات الحديثة. وتضع هذه الأنظمة على المستوى العام جدا شروطاً على جمع واستخدام وتخزين البيانات الشخصية (القواعد التي تنظم المتحكمين في البيانات)، ومنح بعض الحقوق للأفراد الذين ترتبط بهم البيانات (أصحاب البيانات)، وتنفيذ نظام رقابة يضمن مراعاة القواعد والتصدي لأي مخالفة. ومن الجوانب المحورية لجميع أنظمة حماية البيانات تقريبا تحديد المبادئ الأساسية التي تنظم هذه المسائل، وعلى وجه الخصوص جمع واستخدام وتخزين البيانات الشخصية.

وفي إطار منظمة الأمم المتحدة، وضع القرار رقم 95/45، الصادر عن الجمعية العامة بعنوان المبادئ التوجيهية لتنظيم استخدام ملفات البيانات الشخصية المجهزة إلكترونياً،[199] وضع عشرة مبادئ أساسية بشأن حماية البيانات تتصل في المقام الأول بالتشريعات الوطنية، ولكنها ملزمة على المنظمات الدولية، بعد إدخال التعديلات المناسبة. وهي تنطبق على الملفات المجهزة الكترونياً لدى المعنيين من القطاع العام والخاص والمحتوية على بيانات بشأن الأفراد، وقد تمتد لتغطي ملفات يدوية و/ أو أشخاص اعتباريين.

وتتضمن المبادئ التوجيهية عددا من الأسس التي تحكم جمع واستخدام البيانات الشخصية التي توجد في العديد من أنظمة حماية البيانات. ويمكن تلخيص المبادئ الرئيسية منها على النحو التالي:

المشروعية والنزاهة: يجب أن يكون جمع البيانات مشروعاً ونزيها وغير مخالفاً لأغراض ومبادئ ميثاق الأمم المتحدة.

الدقة: يتحمل المتحكمون في البيانات المسؤولية عن التحقق من البيانات بشكل منتظم لضمان صحتها ودقتها، والتأكد من كونها كاملة بقدر الإمكان للغرض الذي جمعت من أجله وذلك لتجنب الأخطاء الناتجة عن السهو.

---

197 المرجع السابق، الفقرة 41.

198 المرجع السابق، الفقرات 46–50.

199 أعتمد في 14 ديسمبر/ كانون الأول 1990، 45/RES/A/95.

التركيز على الغرض: يتعين أن يكون الغرض الذي من أجله تم جمع البيانات غرضاً مشروعاً ويعلم به أصحاب البيانات، ولا ينبغي استخدام البيانات لأغراض أخرى غير متوافقة، وتحفظ البيانات للمدة اللازمة لخدمة هذا الغرض.

وصول الأشخاص المعنيين: لأصحاب البيانات الحق في معرفة وقت جمع البيانات الخاصة بهم أو معالجتها، ولهم الحق في الوصول إلى هذه البيانات في صيغة واضحة دون إبطاء لا مسوغ له أو تكلفة، وللقيام بالتصحيحات المناسبة أو الحذف.

عدم التمييز: أي استثناءات على هذه المبادئ يعتبر تمييزياً في طبيعته.

الأمن: ينبغي اتخاذ التدابير المناسبة لحماية البيانات ضد المخاطر الطبيعية والبشرية على حد سواء، مثل الوصول غير المصرح به أو إساءة الاستخدام أو التلوث المادي.

تقر هذه المبادئ التوجيهية بأنه قد تكون هناك حاجة لوجود استثناءات عن المبادئ الخمسة الأولى، ولكن في إطار ضرورة حماية الأمن القومي أو النظام العام أو الصحة أو الآداب العامة أو حقوق الآخرين وحرياتهم. وتشترط تعيين سلطة رقابية مستقلة تتحمل مسؤولية ضمان احترام تلك المبادئ وتطبيق أنظمة الجزاءات على كل من يخرج عن القواعد. وتقتضي كذلك وضع قيود على تداول المعلومات إلى البلدان التي لا تقدم ضمانات مماثلة.

14) المعايير الإقليمية المتعلقة بحماية البيانات

ثمة العديد من المعايير الإقليمية المتعلقة بحماية البيانات، ومن المنظومات الرئيسية القائمة حالياً ما يلي:

- منظمة التعاون الاقتصادي والتنمية (OECD): المبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية لسنة 1980 بشأن حماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود. [200]
- منتدى التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC): إطار الخصوصية لمنتدى التعاون الاقتصادي لأسيا والمحيط الهادي لسنة 2005.
- الجماعة الاقتصادية لدول غرب أفريقيا (إيكواس): القانون التكميلي رقم A/SA.1/01/10 بشأن حماية البيانات الشخصية داخل إيكواس. [201]
- منظمة الدول الأمريكية (OAS): قرار الجمعية العامة رقم 2661 بشأن الوصول إلى المعلومات العامة وحماية البيانات الشخصية. [202]
- مجلس أوروبا (COE): اتفاقية عام 1981 لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية، [203] بصيغتها المعدلة بالبروتوكول الإضافي لاتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية وفيما يتعلق بالسلطات الإشرافية وتدفقات البيانات عبر الحدود والصادر سنة 2001. [204]

---

200 تم الاعتماد بتوصية مجلس منظمة التعاون الاقتصادي والتنمية في 23 سبتمبر/ أيلول 1980.

201 تم الاعتماد في 16 فبراير 2010.

202 تم الاعتماد في 7 يوليو 2004، /RES.

203 تم الاعتماد في 28 يناير/ كانون الثاني 1981، E.T.S. No. 108، دخلت حيز النفاذ في 1 أكتوبر/ تشرين الأول 1985.

204 تم الاعتماد في 8 نوفمبر/ تشرين الثاني 2001، E.T.S. No. 181، دخل حيز النفاذ في 1 يوليو 2004.

- الاتحاد الأوروبي: التوجيه EC/46/95 للبرلمان الأوروبي والمجلس الأوروبي بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وبشأن حرية حركة تلك البيانات.[205] 3.1.2.2 معايير منتدى التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC)

تجمع عضوية منتدى التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC) بين دول مثل كندا وشيلي وبيرو والولايات المتحدة الأمريكية من جانب المحيط الهادئ، مع عدد من الاقتصادات الآسيوية بما فيها الاقتصادات الكبرى مثل الصين واليابان والاتحاد الروسي، وكذلك إندونيسيا وفيتنام وتايلند، ودول مثل أستراليا ونيوزيلندا.

لقد وضعت القواعد الرئيسية لمنتدى التعاون الاقتصادي لآسيا والمحيط الهادي (APEC) بشأن الخصوصية في إطار الخصوصية الصادر عن المنتدى.[206] ولقد وضعت ديباجة هذا الإطار أسس اعتماده بشكل واضح في ضرورة الحفاظ على ثقة المستهلك وذلك من أجل تعزيز الفوائد الاقتصادية من التجارة الإلكترونية. ويشير المنتدى إلى اتساق الإطار مع المبادئ التوجيهية الصادرة عن منظمة التعاون الاقتصادي والتنمية (OECD)، مع تحقيق التوازن بين الحاجة إلى خصوصية المعلومات واحتياجات الأعمال. كما يقر المنتدى بالحاجة إلى توفير المرونة للدول الفردية فيما يتعلق بالتنفيذ.

تتشابه المبادئ الأساسية تقريباً من حيث الطبيعة مع المبادئ التوجيهية للأمم المتحدة، وكذلك المعايير الأوروبية ومعايير منظمة التعاون الاقتصادي والتنمية. ويتميز الإطار بوجود درجة محددة من المرونة، والتي قد تقارن بالمعايير الأوروبية الأكثر تفصيلا، بما يسمح بإيضاح الاستثناءات بمزيد من التفصيل. وينعكس هذا أيضا في الأحكام المتعلقة بالتنفيذ، والتي تمنح سلطة تقديرية واسعة لاقتصادات الدول الأعضاء لاتخاذ قرار بشأن أفضل نهج متبع.

تحدد المبادئ 'المعلومات الشخصية' على نطاق واسع في صورة جميع المعلومات المتعلقة بالفرد المحدد الهوية أو الذي يمكن تحديد هويته و «المتحكم في المعلومات الشخصية» على نطاق واسع كذلك كشخص يمارس السيطرة أو استخدام المعلومات الشخصية (الفقرات 9–10). وكما نلاحظ، يتضمن الإطار على وجه التحديد درجة من المرونة عند تطبيقه على أساس الفروق الاجتماعية والاقتصادية والثقافية، فضلا عن ضرورة حماية الأمن القومي أو السلامة العامة والسياسة العامة (الفقرات 12–13).

يتمحور المبدأ الموضوعي الأول حول «الوقاية من الضرر»، مما يقتضي اتخاذ تدابير لمنع إساءة استخدام المعلومات الشخصية التي يحتمل أن تزيد من شدة أو خطورة الضرر (الفقرة 14). ويتعين على المتحكمين في المعلومات تقديم إشعار، مسبقاً إن أمكن أو في وقت جمع المعلومات، للأفراد عن حقيقة جمع المعلومات الشخصية وأغراض جمعها وأنواع الأشخاص الذين قد يتم التصريح لهم بتلك المعلومات وكيفية الاتصال بالمتحكم (الفقرات 15–17). ولا يجوز جمع أية معلومات إلا ما اتصل منها بالغرض المعلن، على أن يتم ذلك بالوسائل المشروعة والنزيهة (الفقرة 18).

لا تستخدم المعلومات إلا للأغراض التي جمعت من أجلها أو لأغراض مشابهة، باستثناء موافقة الفرد أو عند ضرورة توفير خدمة يطلبها الفرد (الفقرة 19). وينبغي أيضا تزويد الأفراد بحق الخيار فيما يتعلق بجمع واستخدام المعلومات الخاصة بهم والكشف عنها (الفقرة 20). ويجب أن تتسم المعلومات بالدقة وأن تكون

---

205 تم الاعتماد في 24 أكتوبر/ تشرين الأول 1995، OJ L 281، ص. 31، والمكمل بالتوجيه رقم EC/58/2002 من البرلمان الأوروبي والمجلس بتاريخ 12 يوليو 2002 بشأن معاجلة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات السلكية، OJ L 201، ص. 37، والتوجيه رقم EC/24/2006 للبرلمان الأوروبي والمجلس بتاريخ 15 مارس/ آذار2006 بشأن الاحتفاظ بالبيانات المنشأة أو المعالجة بشأن تقديم خدمات الاتصالات الالكترونية المتاحة بصورة عامة أو شبكات الاتصالات العامة والتوجيه المعدل رقم EC, OJ L/58/2002، ص. 54.

206 متوفر على: http://publications.apec.org/publication-detail.php?pub_id=390.

حديثة، وتخزن بطريقة تقلل إلى أدنى حد من مخاطر الوصول غير المصرح به أو التعديل، وما إلى ذلك (الفقرات 21–22).

يكون للأفراد الحق، تماشيا مع المبادئ الأساسية لحماية البيانات، في الوصول إلى المعلومات الخاصة بهم وتصحيحها بعد استيفاء التكاليف والقيود الأخرى المختلفة (الفقرات 23–25). وأخيرا، يكون المتحكم في المعلومات هو المسؤول عن الامتثال لهذه المبادئ، بما في ذلك عن طريق ضمان التزام كل من تصل إليه المعلومات بهذه المبادئ (الفقرة 26).

3.2.1.3 المعايير الأوروبية

ثمة فروق واسعة بين الأنظمة الإقليمية المختلفة لحماية البيانات، على الرغم من أن نظام الاتحاد الأوروبي يتشابه بشكل كبير مع نظام مجلس أوروبا وتعديلاته. ونحن نقدم لمحة أكثر تفصيلاً عن نظام الاتحاد الأوروبي كمثال على النهج القوي لحماية البيانات وأيضا على نظام له تأثير عالمي واسع النطاق.

إن النظام الذي يطبقه الاتحاد الأوروبي هو نظام معترف به على نطاق واسع وذلك لأنه نظام تقدمي للغاية، من حيث توفير حماية قوية للبيانات، ولأنه يلعب دوراً قيادياً في هذا المجال، من حيث ممارسة النفوذ على قوانين حماية البيانات في البلدان الأخرى. وهذه القواعد ملزمة رسميا على الدول الأعضاء في الاتحاد الأوروبي والبالغة 27 دولة، ولكن تأثيرها يصل إلى أبعد من ذلك بكثير. ففي دراسة حديثة، قام جرينليف (Greenleaf) بمقارنة الأنظمة الأوروبية مع نظام منظمة التعاون الاقتصادي والتنمية (OECD) ونظام منتدى التعاون الاقتصادي للمحيط الهادي وآسيا (APEC)، وتحديد أهم عشرة اختلافات بينهم، والتي عكست جميعها معايير أعلى في النظم الأوروبية. واستنتج بعد تحليله لــ 29 قانون من قوانين حماية البيانات خارج أوروبا أن 13 منها تدرج تسعة على الأقل من هذه الخصائص العشرة الواردة في الأنظمة الأوروبية، وأن 19 لديها سبعة على الأقل وأن 23 لديها خمسة على الأقل أو واحد ونصف.[207] وتوحي هذه العلاقة القوية للغاية بأن الأنظمة الأوروبية كانت ذات نفوذ كبير على الصعيد العالمي.

اعتمد الاتحاد الأوروبي ميثاق الحقوق الأساسية للاتحاد الأوروبي في ديسمبر/ كانون الأول 2000،[208] الذي يحتوي على تدابير حماية قوية للخصوصية بشكل عام (المادة 7) وحماية البيانات على وجه الخصوص (المادة 8)، وتتطلب حماية البيانات أن تكون معالجتها نزيهة ولغرض محدد وعلى أساس الموافقة، حيث إن لأصحاب البيانات الحق في الوصول إلى البيانات الخاصة بهم وتصحيحها، ويجب أن تتولى الرقابة هيئة مستقلة. وعلى الرغم من اعتماد هذا الميثاق بعد أن اعتمدت الأحكام الرئيسية لإطار حماية البيانات، إلا أن هذه الأحكام الأخيرة يجب أن تدرس في ظل هذه الضمانات الأساسية.

إن النهج الأساسي المتمثل في التوجيه 95/46 هو تطبيق القواعد على نطاق واسع للغاية ثم تطبيق بعض القيود أو الاستثناءات. ومن ثم يرد تعريف البيانات الشخصية في المادة الثانية بأنها أي بيانات تتعلق بشخص طبيعي معرف الهوية أو يمكن تعريف هويته، وتعريف المعالجة على أنها أي عملية تتم على البيانات الشخصية (بما في ذلك الجمع والتخزين وما إلى ذلك)، والمتحكم على أنه شخص طبيعي أو اعتباري يحدد أغراض ووسائل معالجة البيانات.

وفقا لهذه التعاريف، ينطبق تعريف «المتحكم» على أي فرد يقوم بتخزين أرقام الهاتف على الهاتف المحمول أو الكمبيوتر. ومع ذلك، تنص المادة 3 على أن التوجيه لا ينطبق على معالجة البيانات لأغراض خارج نطاق قانون الجماعة الأوروبية (والذي يشتمل على الأمن والأنشطة المتصلة بالقانون الجنائي) أو المعالجة من قبل شخص طبيعي لأنشطة "شخصية أو منزلية بحتة". كما أنه يحد من نطاق التوجيه فيقصره على المعالجة

---

207 أنظر على سبيل المثال جرينليف، جي (Greenleaf, G). تأثير المعايير الأوروبية لخصوصية البيانات خارج أوروبا: تداعيات العولمة لاتفاقية 108، جامعة نيو ساوث ويلز، كلية القانون، سلسلة الأبحاث، البحث رقم 42، 2011.

208 2000/364 C/01.

الكلية أو الجزئية بوسائل آلية (معظمها تكون إلكترونيا)، أو على البيانات التي تشكل جزءاً من نظام الإيداع، وبالتالي استبعاد البيانات المخزنة بطريقة مخصصة أو بطريقة غير رسمية.

تنص المادة 6 على مبادئ حماية البيانات (أنظر المربع)، وهي في الأساس ذات المبادئ الثلاثة الأولى المذكورة أعلاه من قرار الجمعية العامة للأمم المتحدة رقم 95/45. وتتسم معظم هذه المبادئ بالوضوح الكافي. ومن واقع التجربة، لا تتعرض قواعد المعالجة المتوافقة للخرق إذا تم استخدام المعلومات "بما يتوقع معه المزودون بالمعومات استخدامها والكشف عنها."[209]

15) المبادئ التوجيه للاتحاد الأوروبي بشأن حماية البيانات

ينص توجيه الاتحاد الأوروبي رقم 95/46 على المبادئ الأساسية لحماية البيانات في المادة 6، وتشترط هذه المبادئ ضرورة مراعاة التعامل مع البيانات الشخصية بالشروط التالية:

(أ) المعالجة النزيهة والقانونية؛

(ب) جمعها لأغراض واضحة ومحددة ومشروعة، وعدم معالجتها بطريقة أخرى غير متوافقة مع تلك الأغراض. ولا تعتبر المعالجة الزائدة للبيانات لأغراض تاريخية أو علمية أو إحصائية غير متوافقة، شريطة أن تقدم الدول الأعضاء الضمانات المناسبة لحمايتها؛

(ج) أن تكون البيانات كافية ومتصلة بالغرض الذي جمعت أو تعالج من أجله وعدم زيادتها عنه؛

(د) أن تكون دقيقة، وأن يتم تحديثها عند الضرورة؛ ويراعى اتخاذ كل ما هو معقول من خطوات لضمان مسح أو تصحيح البيانات غير الدقيقة أو غير الكاملة، مع الأخذ في الاعتبار الأغراض التي جمعت أو التي يتم معالجتها من أجلها؛

(هـ) الاحتفاظ بها في شكل يسمح بتحديد صاحب البيانات لمدة لا تزيد عما هو ضروري للأغراض التي جمعت من أجلها أو يتم معالجتها من أجلها. ويتعين على الدول الأعضاء وضع الضمانات المناسبة للبيانات الشخصية المخزنة لفترات أطول للاستخدام التاريخي والإحصائي أو العلمي.

تضع المادة 7 من التوجيه 95/46 شروط توضح متى يمكن معالجة البيانات، والتي تشمل بموافقة صاحب البيانات، أغراض إبرام العقود مع صاحب البيانات، ومتى يكون من الضروري امتثال المتحكم للالتزامات القانونية، ومتى يكون من الضروري حماية «المصالح الحيوية» للشخص المعني (مثل جمع الدم بعد وقوع حادث)، ومتى يكون من الضروري للمصلحة العامة أو في إطار ممارسة السلطة الرسمية، أو متى تكون الضرورة لحماية المصالح المشروعة للمتحكم أو لطرف ثالث، وذلك بشرط أن يتوافق ذلك مع مصالح صاحب البيانات. وفي السببين الأخيرين، قد يعترض صاحب البيانات على معالجتها «لأسباب مشروعة ومقنعة»، وينص التوجيه على حق الاعتراض على معالجة البيانات لأغراض التسويق المباشر (المادة 14). وسيكون من الواضح على الفور أن هذه القائمة هي قائمة واسعة بطبيعتها وتخضع للتأويلات فضفاضة وربما متباينة.

تمثل موافقة صاحب البيانات جزءاً رئيسياً من النظام ويجب أن تكون واضحة لا لبس فيها. ومع ذلك، يتحقق هذا المعيار عند تحرير اتفاقية بشروط وأحكام خاصة، مثل اتفاقيات الخدمات القائمة على الإنترنت. وهذا هو الحال في معظم الأحيان عندما لا يقوم صاحب البيانات بقراءة الشروط والأحكام، وربما يجد

---

209 لجنة حماية البيانات الايرلندية، قاعدة حماية البيانات رقم 3: استخدام وزيادة معالجة المعلومات الشخصية. متوفر على: http://dataprotection.ie/viewdoc.asp?DocID=25.

صعوبة في فهمها. ويمكن اعتبار ذلك بمثابة عبء لا مبرر له على أصحاب المعلومات، على الرغم من أن الفكرة الكاملة للسيطرة على بيانات الفرد تؤدي ربما حتماً إلى هذا.

تحدد المواد من 10 إلى 12 من التوجيه بعض الحقوق الخاصة بصاحب البيانات. فوفقا للمادتين 10 و 11، يجب إبلاغ صاحب البيانات بهوية المتحكم (أو من ينوب عنه)، وبأغراض معالجة البيانات، والمعلومات المختلفة عند الضرورة لضمان معالجة عادلة مثل مستلمي البيانات والحق في الوصول إلى البيانات وتصحيحها. ويخفف من صرامة هذه الشروط إلى حد ما القاعدة التي تنص على عدم ضرورة توفير المعلومات إذا كانت لدى صاحبها بالفعل، ويمكن بالموافقة استخدام الشروط والأحكام العامة «لنقل» هذه المعلومات إلى صاحبها. وعلاوة على ذلك، إذا تمت المعالجة من قبل هيئة لم تجمع البيانات، فإنه ليست هناك حاجة إلى توفير هذه المعلومات في حالة البحث التاريخي أو العلمي، حيث إن هذا يكون مستحيلاً أو غير مناسباً، أو عندما تكون المعالجة بحكم القانون.

وفقاً للمادة 12، يحق لأصحاب البيانات الحصول على ما يلي من المتحكم على فترات معقولة ودون تأخير مفرط أو تكلفة زائدة:

- تأكيد على ما إذا كان يتم معالجة البيانات، والغرض من ذلك وفئات البيانات والمستلمين لها؛
- البيانات بشكل واضح بالإضافة إلى مصدرها؛
- المنطق المستخدم في أي عملية معالجة تلقائية، وعلى الأقل عندما يؤدي ذلك إلى قرار يمس صاحب البيانات.

كما يتعين على المتحكمين كذلك تصحيح أو مسح أو غلق البيانات التي لم يتم فيها الالتزام بالتوجيه، ولا سيما بسبب عدم اكتمال البيانات أو انتفاء دقتها، ويتعين عليهم إخطار الأطراف الثالثة المعنية بهذا. وتنص المادتان 16 و 17 على وجوب حفظ ومعالجة البيانات بطريقة آمنة.

تسمح المادة 13 للدول بأن تحد من الالتزامات المنصوص عليها في المواد 6 و 10 و 11 و 12 و 21 (أنظر أدناه) عند وجود ضرورة لحماية الأمن القومي أو النظام العام، أو لمنع انتهاكات جنائية أو مهنية، أو لأسباب اقتصادية مهمة، أو لأغراض المراقبة أو التنظيم، أو لحماية صاحب البيانات أو حقوق الآخرين أو حرياتهم.

من القواعد الأخرى الصارمة، وإن كان لها استثناءات تخفف من صرامتها، التزام المتحكم بإعلام هيئة الرقابة (قبل معالجة البيانات) بالغرض من المعالجة وفئات أصحاب البيانات والمستلمين لها وأي عمليات نقل مقترحة إلى بلدان ثالثة. ويجب حفظ سجل بجميع عمليات المعالجة التي أبلغ عنها بهذه الطريقة لدى هيئة الرقابة ويكون متاحاً للجمهور العام.[210] ويجوز للدول وضع استثناءات واضحة لهذا الشرط، بما في ذلك المنظمات غير الربحية، حيث يقوم المتحكمون بتعيين مسؤولين لحماية البيانات، وبالنسبة للسجلات التي ينص عليها القانون بهدف توفير المعلومات للجمهور، وبالنسبة لفئات معينة من المعالجة التي لا يحتمل أن تضر بالحقوق أو الحريات. ويشترط في عملية المعاجلة التي يشملها الاستثناء أن تتوفر المعلومات الرئيسية لأي فرد عند الطلب (المواد 18 و 19 و 21).

---

210 مثال على ذلك سجل المتحكمين في البيانات في المملكة المتحدة، متوفر في صيغة قابلة للبحث على: http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

16) نظرة عامة على نظام الاتحاد الأوروبي لحماية البيانات

- العناصر الرئيسية لهذا النظام:
- تعاريف فضفاضة للبيانات الشخصية ومعالجة البيانات؛
- المبادئ التي تحكم البيانات الشخصية: المعالجة النزيهة، ولأغراض محددة، وكفاية البيانات واتصالها بموضوع المعالجة وعدم زيادتها عنه، ودقتها وتحديثها وعدم الاحتفاظ بها أكثر من اللازم؛
- حقوق أصحاب البيانات: إخبارهم بالمتحكم والغرض من المعالجة، وحصولهم على البيانات في شكل واضح، وإمكانية تصحيحهم أو حذفهم للبيانات
- التزام المتحكم بإخطار هيئة الرقابة، وحفظ هذه الإخطارات في سجل عام
- سبل الانصاف المتاحة لأصحاب البيانات
- نقل البيانات عند توافر الحماية الكافية فقط
- الرقابة من جانب هيئة مستقلة

ثمة العديد من سبل الانصاف المتوفرة لصاحب البيانات بما في ذلك حقه في الحصول على تعويض من المتحكم عند تعرضه للضرر بسبب المعالجة غير القانونية للبيانات (المادة 23) وإلى سبل الانصاف القضائية عند انتهاك حقوقه (المادة 22). ويجب أيضاً فرض عقوبات على كل من يخالف هذه القواعد (المادة 24).

من الأجزاء الأساسية للتوجيه تلك القيود التي يفرضها على عمليات نقل البيانات التي يتم معالجتها إلى بلدان خارجية (أي خارج الاتحاد الأوروبي) (المادة 25). ولا يمكن أن يتم هذا إلا إذا عرضت تلك البلدان «مستوى كاف من الحماية» للبيانات. ولكن، في حالات استثنائية، يجوز للدول أن تسمح بتحويل البيانات إلى البلدان التي لا توجد فيها حماية كافية لأسباب تشبه إلى حد كبير تلك الأسباب المنطبقة على معالجة البيانات المشروعة في المقام الأول، باستثناء الأول منها (أي مصالح المتحكم أو الطرف الثالث) (المادة 26).

قد تقوم اللجنة بالتصديق على أن جميع الدول توفر الحماية الكافية. وقد تم ذلك بالنسبة لدول مثل سويسرا وكندا والأرجنتين.[211] وفي حالة الولايات المتحدة الأمريكية والتي لا تصل إلى مستوى "الدول ذات الحماية الكافية" بسبب افتقارها إلى التشريعات التي تنظم حماية البيانات المركزية لجهات خاصة، وضعت وزارة التجارة برنامج دولي لاعتماد مبادئ خصوصية الملاذ الآمن.[212] وهو عبارة عن برنامج تطوعي يمكن للشركات التقدم إليه للحصول على اعتماد في حال امتثالها لمبادئ الملاذ الآمن السبعة. وهذه المبادئ تتماشى مع القواعد الأوروبية لحماية البيانات، وتشتمل على تقديم إشعار حول أغراض جمع البيانات وحق الأفراد في رفض نقل البيانات إلى أطراف ثالثة أو استخدامها لأغراض أخرى، ومتطلبات أمن للبيانات وما إلى ذلك.[213] وبمجرد الحصول على الاعتماد، يتم قبولها على أنها توفر الحماية الكافية للبيانات الشخصية لأغراض قواعد الاتحاد الأوروبي.[214]

---

211 أنظر : http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm

212 أنظر http://export.gov/safeharbor

213 تتوفر قائمة كاملة من المبادئ على http://export.gov/safeharbor/eu/eg_main_018475.asp

214 تم اعتماد النظام لدى اللجنة الأوروبية في القرار رقم 2000/520/CE. أنظر http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

ينص التوجيه على نوعين من الهياكل المؤسسية. أولاً، يجب على كل طرف إنشاء هيئة مستقلة إشرافية أو رقابية بصلاحيات مختلفة مثل التحقيق والتدخل، بما في ذلك عن طريق حظر معالجة البيانات، ومباشرة الإجراءات القانونية والاستماع إلى الشكاوى (المادة 28). ثانيا، هناك ما يسمى بفريق عمل المادة 29، ويتألف من ممثلين بالهيئات الرقابية ويكون دورهم أساساً دوراً استشارياً في طبيعته (المواد 29 و 30).

ليس من شك في أن للتوجيه دور هام جداً في حماية البيانات الشخصية. ولقد أشاد به الكثيرون على نطاق واسع لكونه محايد من حيث التكنولوجيا (أي أنه ينطبق بغض النظر عن التكنولوجيا المستخدمة لمعالجة البيانات)، ولفرض معايير عالية تقوم على مبادئ مرنة، وللتقريب بين القواعد عبر الاتحاد الأوروبي، وأكثر من ذلك.

ولكن انتقده البعض في الوقت نفسه لكونه قد عفا عليه الزمن (مفهوم في ظل وتيرة التغير السريعة في معالجة البيانات الشخصية) ويتسم بالبيروقراطية المفرطة، والجمود والإلزام وعدم التركيز الكافي على المخاطر بدلا من الإجراءات، بل وعدم الواقعية (وعلى سبيل المثال فيما يتعلق بالنقل الدولي للبيانات في سياق التدفقات الواسعة والعالمية للبيانات).[215]

ومن ثم هناك قبول واسع النطاق للحاجة إلى تجديد التوجيه وهناك مشاورات جارية بهدف تحقيق ذلك. وتصف المفوضية الأوروبية أهداف هذه العملية بأنها ترمي إلى تحديث النظام لمواجهة تحديات العولمة والتكنولوجيات الجديدة، ولتعزيز الحقوق مع تقليل الإجراءات الإدارية، ولضمان التدفق الحر للبيانات، ولتحسين وضوح واتساق القواعد، ولتحقيق التنفيذ المتسق والفعال.[216]

في 25 يناير/ كانون الثاني 2012، أصدرت الجنة مقترحاتها 'النهائية' لما تقترح تحويله إلى تنظيم (بدلاً من توجيه) بشأن حماية البيانات.[217] وتكمن الأهمية الرئيسية لذلك في أن القواعد سيكون له أثر قانوني مباشر في كل دولة عضو.[218] تتضمن المقترحات عددا من الأحكام التي من شأنها أن تشدد قواعد التوجيه القائم وتزيل الغموض عن بعض المسائل الملتبسة وتعاريف معينة، و "تدعيم" مختلف النظم، مثل تزويد أصحاب البيانات بالمعلومات، وإجراءات ممارسة صاحب البيانات لحقوقه، وسبل الانصاف وصلاحيات الرقابة والتعاون.

ويقترح مشروع التنظيم أيضاً عدداً من القواعد الجديدة. حيث يجب أن تكون المعلومات التي تقدم إلى أصحاب البيانات شفافة ويمكن الوصول إليها بسهولة ومفهومة. وهناك قاعدة أخرى تنص على الحق في حمل البيانات، بما في ذلك الحق في الحصول على نسخة من بيانات الفرد في تنسيق مستخدم بشكل شائع. ويتعين على المتحكمين وضع سياسات وآليات داخلية لضمان الامتثال بالتزاماتها، والإبلاغ عن مخالفات البيانات وإجراء عمليات التقييم قبل المعالجة التي تنطوي على المخاطر. ويتعين على الهيئات العامة والهيئات الخاصة الكبيرة تعيين موظفي حماية البيانات. كما أن مشروع التنظيم سوف ينشئ هيئة جديدة باسم

---

215 أنظر على سبيل المثال روبينسون، إن (Robinson, N.)؛ جروكس، إتش (Graux, H.)؛ بوترمان إم (Botterman, M.)، وفاليري إل (Valieri, L.). مراجعة توجيه الاتحاد الأوروبي لحماية البيانات: ملخص، معد لمكتب مفوض المملكة المتحدة المعني بالمعلومات، مايو 2009، تمهيد. متوفر على http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf

216 أنظر http://ec.europa.eu/justice/policies/privacy/review/index_en.htm

217 مقترح تنظيم البرلمان الأوروبي والمجلس بشأن حماية الأفراد فيا يتعلق بمعالجة البيانات الشخصية وحركة تلك البيانات بحرية (تنظيم حماية البيانات العامة)، بروكسل، 25/1/2012، COM(2012) 11 final, 2012/0011 (COD).

218 التوجيه بالمقارنة لا يلزم إلا الدول الأعضاء على توافق القانون مع أحكامها.

مجلس حماية البيانات الأوروبي، وذلك لاستبدال فريق عمل المادة 29، مع منحه سلطات موسعة. ويتضمن التنظيم كذلك توضيحاً لقواعد 'كفاية' البيانات لأغراض التحويلات إلى البلدان غير الأعضاء.

إن بعض المقترحات قد تكون أكثر إثارة للجدل. على سبيل المثال، يقترح التنظيم الجديد التطبيق على كل عمليات معالجة البيانات القائمة خارج الاتحاد الأوروبي، «حيث يتم توجيه أنشطة معاجلة البيانات لأصحابها، أو تعمل على مراقبة سلوك أصحاب تلك البيانات». وقد ينشئ هذا التنظيم "الحق في العفو"، بما في ذلك الحق في طلب محو كافة البيانات ووضع حد لأي معالجة أخرى.

4.2.1.3. قواعد تكميلية

جاء التوجيه 95/46 مكملاً بتوجيهين، وهما التوجيه رقم 2002/58 بشأن حماية الخصوصية في الاتصالات الإلكترونية (توجيه الخصوصية الالكترونية) والتوجيه 200رقم 6/24 بشأن الاحتفاظ بالبيانات (توجيه الاحتفاظ بالبيانات).[219] وينص التوجيه السابق على عدد من القواعد الخاصة فيما يتعلق بالخصوصية في سياق الاتصالات الالكترونية، ويتطلب سرية الاتصالات وأنواع أخرى مختلفة من البيانات (بيانات الانتقال وبيانات الموقع)، إلا لأغراض محدودة – مثل التحصيل والتسويق وخدمات القيمة المضافة – وينص على حقوق المستخدم فيما يتعلق بالمسائل المتعلقة بالاتصالات – مثل تبويب الفواتير، وخدمات تحديد هوية المتصل، وتحويل المكالمات، وأدلة المشتركين والاتصالات غير المرغوب فيها. ويجوز للدول من خلال التدابير التشريعية تجاوز القواعد الخاصة بالسرية لأغراض الأمن القومي والمصلحة العامة والتحقيق في الجرائم – والتي تخرج جميعها عن اختصاص الاتحاد الأوروبي – بما في ذلك اشتراط الاحتفاظ بالبيانات.

يفرض توجيه الاحتفاظ بالبيانات في الأساس شروطاً صارمة على هذه القواعد عن طريق اشتراط الاحتفاظ بعدد كبير من فئات بيانات الاتصالات – باستثناء محتوى الاتصالات – لمدة تتراوح بين ستة أشهر وسنتين، كاستثناء من الأحكام ذات الصلة المعنية بعدم الاحتفاظ بالبيانات في توجيه الخصوصية الالكترونية.

17) الأحكام الدستورية بشأن توجيه الاحتفاظ بالبيانات للاتحاد الأوروبي[220]

ألغت محاكم ثلاث دول – وهي جمهورية التشيك وألمانيا ورومانيا – القواعد الوطنية بشأن الخصوصية التي ترمي إلى تطبيق توجيه الاتحاد الأوروبي للاحتفاظ بالبيانات على أساس أنها غير دستورية. ففي أكتوبر/ تشرين الأول 2009، قضت المحكمة الدستورية الرومانية بأن التوجيه يخالف المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان. وأشارت المحكمة من بين أمور أخرى إلى الطبيعة الشمولية لمطلب الاحتفاظ بالبيانات لأنه ينطبق على الجميع، سواء كانوا قد ارتكبوا جرم بالفعل أو يشتبه ارتكابهم هذا الجرم. وقالت المحكمة بأن نطاق التوجيه يكتنفه الغموض وأن القواعد تفتقر إلى الضمانات الكافية ضد سوء الاستخدام. [221] ويمثل القرار أهمية خاصة بقدر

---

219 الحاشية 205.

220 المعلومات الواردة في هذا القسم مقتبسة من تقرير تقييم شادو لدى منظمة الحقوق الرقمية الأوروبية (EDR) بشأن توجيه الاحتفاظ بالبيانات (2006/24/17 ،(EC إبريل 2011، متوفر على: /http://www.edri.org/files shadow_drd_report_110417.pdf والتقرير الرسمي الصادر عن اللجنة إلى المجلس والبرلمان الأوروبي: تقرير تقييم بشأن توجيه الاحتفاظ بالبيانات (التوجيه رقم 2006/24/EC)، بروكسل، 18/4/2011 COM(2011) 225 نهائي.

221 القرار رقم 1258 من 8 أكتوبر/ تشرين الأول 2009 للمحكمة الدستورية بأرمينيا، المرصد الأرميني الرسمي رقم 789، 23 نوفمبر/ تشرين الثاني 2009. متوفر على- http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

ما يحمله من دلاله استنادا إلى المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان. فلو أيدت المحكمة الأوروبية لحقوق الإنسان هذا التفسير، فإن هذا يعني مواجهة دول الاتحاد الأوروبي لمأزق قانوني.

وفي مارس/ آذار من عام 2010 حزت المحكمة الدستورية الاتحادية الألمانية نفس هذا الحزو عندما أقرت بانتهاك الأحكام التنفيذية الألمانية للحق في سرية الاتصالات المنصوص عليه في الدستور. وأشارت إلى أن القواعد من شأنها أن تشعر المواطنين بتعرضهم الدائم للمراقبة، الأمر الذي يفسد عليهم التمتع بالحقوق الأساسية المختلفة. أما الاحتفاظ بالبيانات في حدود معينة بغرض حماية المصالح الأمنية الهامة قد يكون له ما يبرره، ولكن القواعد الحالية كانت مبالغة جدا. وأشارت المحكمة أيضا إلى عدم وجود ضمانات، وبوجه خاص عدم وجود الرقابة المناسبة.[222]

وقضت المحكمة الدستورية التشيكية أيضاً في مارس/ آذار2011 أنه نظرا لكثافة واتساع نطاق التدخل في الخصوصية لا يمكن تبرير القواعد على أنها قيد لازم على الحق في الخصوصية. وأشارت في هذا الصدد إلى أن الاحتفاظ بالبيانات التي تشترطها القواعد لم تؤثر كثيراً على إحصاءات الجريمة، وخصوصاً في ظل الإمكانيات التكنولوجية الجديدة التي تساعد على تجنب الكشف عن الهوية. وأشارت المحكمة التشيكية، مثلما فعلت المحكمة الألمانية، إلى أن الأغراض التي تبرر الاحتفاظ بالبيانات هي أغراض واسعة جداً ولا يوجد ضمانات كافية.[223]

وفقاً للجنة الأوروبية: «رفعت كذلك دعاوي الاحتفاظ بالبيانات أمام المحاكم الدستورية في بلغاريا، مما أدى إلى إعادة النظر في قانون نقل البيانات في قبرص بالحكم بعدم دستورية أوامر المحكمة الصادرة بموجب القانون، وفي المجر حيث تنظر المحكمة في قضية تتعلق بالإغفال في قانون النقل للأغراض القانونية لمعالجة البيانات.[224]»[225]

لقد كان التوجيه موضع انتقادات واسعة من المجتمع المدني والأجهزة الرسمية للجنة على حد سواء. فعلى سبيل المثال، وصف مراقب حماية البيانات الأوروبية التوجيه بأنه: "الأداة الأكثر تعدياً على الخصوصية في تاريخ الاتحاد الأوروبي".[226] وذكرت منظمة الحقوق الرقمية الأوروبية (EDRI): "على مدى السنوات الخمس الماضية، أثبت أن توجيه الاحتفاظ بالبيانات بأنه انتهاك غير ضروري وغير مسبوقة للحقوق الأساسية لــ 500 مليون أوروبي».[227] وألغت المحاكم في ثلاثة بلدان - كرواتيا وألمانيا ورومانيا – التشريع التنفيذي للتوجيه على أنه غير دستوري، وتعرض التوجيه لهجوم دستوري في بلدان أخرى أيضا (انظر المربع). وقد أوصت منظمة الحقوق الرقمية الأوروبية (EDRI) بدلا من ذلك "بنظام المحافظة السريعة وجمع بيانات التنقل

---

222 قرار المحكمة الدستورية الاتحادية رقم 1 BvR 256/08، بتاريخ 2 مارس/ آذار2010، متوفر على http://www.bverfg.de/en/press/bvg10- 011en.html

223 الجريدة الرسمية بتاريخ 1 إبريل 2011، قرار المحكمة الدستورية بتاريخ 22 مارس/ آذاربشأن أحكام القسم 97 الفقرة 3 والفقرة 4 من القانون رقم 127/2005 Coll.، بشأن الاتصالات الالكترونية وتعديل بعض القوانين ذات الصلة وتعديلاتها، والمرسوم رقم 485/2005 Coll. بشأن الاحتفاظ بالبيانات ونقلها إلى الجهات المختصة. متوفر على http://www.concourt.cz/clanek/GetFile? id=5075

224 المحكمة الإدارية العليا في بلغاريا، القرار رقم 13627، 11 ديسمبر/ كانون الأول 2008؛ محكمة الاستئناف العليا في قبرص، القضية رقم 65/2009، 78/2009 و15/2010–22/2010، 1 فبراير 2011؛ رفعت الدعوى الدستورية البلغارية من جانب اتحاد الحريات المدنية البلغاري بتاريخ 2 يونيو 2008.

225 تقرير من اللجنة إلى المجلس والبرلمان الأوروبي: تقرير تقييمي حول توجيه الاحتفاظ بالبيانات (التوجيه رقم 2006/24/EC) الحاشية رقم 220، صفحات 20-21.

226 أنظر خطابه بتاريخ 3 ديسمبر/ كانون الأول 2010. متوفر على http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf.

227 تقرير تقييم Shadow بشأن توجيه الاحتفاظ بالبيانات (2006/24/EC)، الحاشية 220، ص 2.

المستهدفة التي تساعد في تحقيقات محددة ('المحافظة على البيانات')، كما تم الاتفاق عليه دولياً في اتفاقية عام 2001 بشأن الجريمة الالكترونية لدى مجلس أوروبا».[228]

ويختلف في ذلك تقرير اللجنة إلى المجلس والبرلمان الأوروبي: تقرير التقييم بشأن توجيه الاحتفاظ بالبيانات (التوجيه رقم EC/24/2006)، والتقييم الرسمي للجنة بشأن التوجيه. حيث يذكر بأن: «أظهر التقييم أن الاحتفاظ بالبيانات هو أداة قيمة لنظم العدالة الجنائية وتنفيذ القانون في الاتحاد الأوروبي» و: «أنه ينبغي أن يستمر الاتحاد الأوروبي من خلال قواعد مشتركة لضمان تطبيق معايير عالية للتخزين والاسترجاع والاستخدام للبيانات المتعلقة بالتنقل والمواقع.»[229] ونتيجة لذلك، فهي تقترح تعديلات على الإطار الحالي للاحتفاظ بالبيانات بدلا من إلغاءه.

في عام 2009، تم اعتماد توجيه جديد بتعديل وتمديد بعض الأحكام في توجيه الخصوصية الالكترونية.[230] لقد عزز التوجيه الصادر عام 2009 من قواعد الأمن وإشعار المستخدمين في حالة أي خرق للأمن، وعزز من وسائل الانصاف والعقوبات المفروضة على مخالفة القواعد. ولكن التغيير الأكثر أهمية كانت تحمله بضع كلمات في المادة 5 (3)، والتي تعني بأنه يجوز القيام بأنشطة التخزين أو الوصول إلى المعلومات على الأجهزة الطرفية للمستخدم بشرط موافقة المستخدم. قبل ذلك كان يكفي تزويد المستخدمين بمعلومات واضحة وشاملة عن تخزين والوصول إلى الجهاز الطرفي، وإعطاءهم الفرصة لرفض هذه الأنشطة.

إن الاسم غير الرسمي للتوجيه هو «توجيه ملفات تعريف الارتباط أو cookie directive»، وذلك بسبب التأثير الهائل الذي ينتج عنه تنفيذ هذه القاعدة على طريقة تشغيل ملفات تعريف الارتباط. ولقد تسبب في رد فعل كبير من المعنيين الذين يعتقدون أنه سيكون من الصعب والمكلف وغير العملي تنفيذه.[231] كما أثارت القاعدة الكثير من التساؤلات عما يمثل الموافقة بالضبط. على سبيل المثال، هل يعتبر المستخدم موافقاً عند ضبط متصفح الإنترنت لقبول ملفات تعريف الارتباط، كما كان الحال في الماضي؟ لا يفترض ذلك، ولكن لن يكون من العملي أيضاً أن يطلب من المستخدمين قبول كل محاولة لوضع ملف تعريف ارتباط على أجهزتهم.

يظل التوجيه بمثابة القانون وتعمل البلدان على تنفيذه (كان الموعد النهائي في شهر مايو/ أيار 2011؛ انظر أدناه للتعرف على الجهود الفرنسية). وفي المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية اعتُمد قانون – وكانت المملكة المتحدة هي الأولى في هذا المضمار- ولكن أشار مكتب مفوض المعلومات المسؤول عن التنفيذ إلى أن القانون سيعطي الشركات مهلة سنة كاملة حتى تمتثل إليه (أي أنه لن يحاكم على أي انتهاكات لمدة سنة).[232] وبالتالي لم يخرج الأثر الحقيقي لهذا الإجراء إلى النور بعد.

---

228 المرجع السابق، ص 6.

229 الحاشية 220، ص 1.

230 التوجيه رقم EC/136/2009 للاتحاد الأوروبي والمجلس بتاريخ 25 نوفمبر/ تشرين الثاني 2009 بتعديل التوجيه رقم EC/22/2002 بشأن الخدمة العامة وحقوق المستخدمين المتعلقة بشبكات الاتصالات والخدمات الالكترونية. التوجيه رقم EC/58/2002 في شأن معالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الالكترونية والتنظيم (EC) رقم 2004/2006 بخصوص التعاون بين السلطات القومية المسؤولة عن تنفيذ قوانين حماية المستهلك. OJ L337، ص 11.

231 أنظر http://online.wsj.com/article/SB10001424052748704444304575628610624607130.html.

232 أنظر http://econsultancy.com/us/blog/8210-q-a-lbi-s-manley-on-preparing-for-the-eu-cookie-laws.

3.2. الحماية الوطنية للخصوصية

1.2.3. الصين

إن نطاق حماية الخصوصية في الصين هو نطاق محدود مع غياب ضمانات دستورية مكتملة أو قانون معني بالخصوصية أو قانون لحماية البيانات. وبشكل عام تمارس السلطات الصينية قدراً كبيراً من السيطرة على الإنترنت ولا يحظى الأفراد إلا بقدر قليل جداً من حماية الخصوصية.[233]

ومع ذلك، ثمة ضغط متزايد من أجل التغيير وخاصة فيما يتعلق بالتهديدات التي تتعرض لها الخصوصية من جهات خاصة. وقد كان الدافع وراء هذا في المقام الأول الانتهاكات التي لحقت بالبيانات الخاصة في صور التسويق المستهدف من المعاملات التجارية، مثل شراء سيارة أو تأمين أو فتح حساب مصرفي. ودائما ما كان يتم ذلك في صورة تدخلية جداً من الرسائل النصية المستهدفة أو المكالمات.

واستجابة لذلك، كان هناك بعض المقترحات القانونية والتنظيمية التي درست أو اعتمدت في السنوات الأخيرة. ووضعت التعديلات المدخلة على القوانين الجنائية وقوانين العقوبات الإجراءات المستقلة لحماية الخصوصية، وكانت هناك مقترحات مختلفة بشأن حماية البيانات.

وعلى عكس العديد من الدساتير، لا يتضمن الدستور الصيني حقاً عاماً قائما بذاته للخصوصية. وتنص المادة 40 من الدستور على ما يلي:

حرية وخصوصية مراسلات مواطني جمهورية الصين الشعبية مكفولة بالقانون. ولا يجوز لأية منظمة أو فرد، لأي سبب من الأسباب، أن ينتهك حرية وخصوصية المراسلات الخاصة بالمواطنين، إلا في حال تلبية احتياجات أمن الدولة أو التحقيق الجنائي أو الأمن العام أو أجهزة النيابة التي يسمح لها فرض رقابة على المراسلات وفقا للإجراءات التي يقررها القانون.[234]

وهذا يؤسس لحق محدود ومقصور في الخصوصية يتعلق فقط بالمراسلات. ورغم ذلك يتعرض لاستثناءات واسعة النطاق، والتي لا تكون ملزمة إلى بما يقرره القانون. وتنص المادة 38 من الدستور على حماية عامة للكرامة الشخصية للمواطنين، وتنص على أنه يحظر "القذف والتشهير والافتراء والاتهام الكاذب". وفسرت المحاكم هذا على أنه ضمان لأساس عام يقوم عليه الحق في الخصوصية، باعتباره متصل بمفهوم أوسع من السمعة. وقد استخدمت حماية السمعة المنصوص عليها في المادة 101 من المبادئ العامة للقانون المدني لسنة 1986 [235] كأساس لحماية الخصوصية أيضاً. ولكن لا يتم ذلك إلا في حال الانتهاكات الجسيمة للسمعة، ومن ثم فإن نطاق حماية الخصوصية في حد ذاتها يكون ضيقاً.

أضاف التعديل السابع على القانون الجنائي بعض الأحكام الجنائية بشأن الخصوصية. ويحظر على العاملين في الهيئات العامة أو المالية ومنظمات الاتصالات السلكية واللاسلكية وهيئات النقل والتعليم أو الهيئات الطبية بيع المعلومات الشخصية التي حصلوا عليها أثناء تأدية عملهم أو نشرها بأي صورة غير مشروعة. ويعاقب بالسجن كل من يخالف ذلك لمدة لا تقل عن ثلاث سنوات، شريطة أن يكون السلوك قد بلغ مستوى معين من الشدة. ويعرض لذات العقوبة كل من يحصل على هذه المعلومات عن طريق السرقة أو أي وسيلة أخرى غير مشروعة، وكذلك بشرط أن يكون السلوك قد بلغ مستوى معين من الشدة. وتعرض المنظمات المرتكبة

---

233 أنظر على سبيل المثال التقارير الصادرة في هذا الصدد من جانب مقررون بلا حدود، في: http://en.rsf.org/china.html؛ منظمة IFJ Press Freedom في الصين، نشرات الحملة، متوفر على: http://asiapacific.ifj.org/en/pages/asia-pacific-china-bulletin-2008؛ والفصل المتعلق بالصين ولا سيما بالمراقبة في الخصوصية وحقوق الإنسان 2006، الحاشية 119، ص 335.

234 متوفر على: http://www.npc.gov.cn/englishnpc/Constitution/node_2825.htm

235 تم اعتمادها في 12 إبريل 1986. متوفر على: http://en.chinacourt.org/public/detail.php?id=2696.

لهذا الجرم لعقوبات مالية، ويعاقب مديريها وموظفيها الآخرين بذات العقوبة المقررة لمن يرتكب هذه الجرائم.[236]

وهذا أمر مهم كونه يمثل أول مبادرة مستقلة للتصدي لانتهاكات الخصوصية في الصين. وفي الوقت نفسه، لا يختلف عن العديد من القوانين الوطنية في الصين من حيث الصياغة العامة إلى حد كبير وعدم وضع تعريف محدد للمصطلحات الرئيسية. ويشتمل هذا على "المعلومات الشخصية"، والوسائل الأخرى غير القانونية لنشر المعلومات، ومستوى الشدة الذي يستوجب المسؤولية. وجاءت أول إدانة بموجب هذه الأحكام في 3 يناير/ كانون الثاني 2010 لدى إحدى المحاكم في تشوهاى بسبب بيع سجل المكالمات الهاتفية من جانب مسؤول كبير في الحكومة وشراءه لاحقاً.

حدث تطور آخر كبير عند اعتماد قانون المسؤولية التقصيرية في 26 ديسمبر/ كانون الأول 2009، والذي دخل حيز النفاذ في 1 يوليو/ تموز 2010، ووضع مسؤولية تقصيرية منفصلة تتعلق بالخصوصية، مما نتج عنه الإدعاء بالحق الخاص عن الأضرار. ويجوز للطرف المدعي لخرق الخصوصية أن يطالب بأرباح قد حققت، أو التعويض عن أضرار نفسية. فمشغل موقع الإنترنت الذي يصبح على علم أو يتم إبلاغه بانتهاك خصوصية طرف آخر أو حقوق أخرى نتيجة لمحتوى يتم استضافته على موقعه الإلكتروني ويعجز عن إزالة هذا المحتوى يعتبر مسؤولاً بالتضامن والتكافل مع الشخص الذي نشر هذا المحتوى. وإذا طلب الطرف المتضرر معلومات التسجيل الخاصة بالطرف الذي قام بالنشر، فإما أن يقوم مشغل الموقع بتوفير تلك المعلومات أو سيصبح مسؤولاً عن المحتوى مسؤولية مباشرة. ولهذه القواعد إشكالية من منظور حرية التعبير بسبب (من بين أمور أخرى) أنها لا تحتاج إلى أي دليل على أن المحتوى يخرق الخصوصية قبل إزالته. وأخيرا، يمكن مقاضاة المؤسسات الطبية عن الأضرار إذا كانت هي المسؤولة عن الكشف غير المصرح به لسجلات المرضى الطبية.[237]

وهذا يمثل امتداداً هاماً من الحماية الجنائية التي اعتمدت سابقاً. ومن الأهمية بمكان أنها تمنح للفرد الحق في التقاضي لحماية حقه في الخصوصية.

كانت هناك بعض المقترحات لسن قانون مكتمل يعنى بحماية البيانات في الصين، إلا أن ذلك لم يؤتي ثماره بعد. في 2006– 2007، تم دراسة قانون حماية المعلومات الشخصية الذي أعده معهد الحقوق في الأكاديمية الصينية للعلوم الاجتماعية وذلك أمام لجنة المعلوماتية التابعة لمجلس الدولة. بيد أن اللجنة لم تعد موجودة. ويصف جرينليف (Greenleaf) الوضع على النحو التالي:

---

236 ترجمة غير سمية للنص من الصينية إلى الإنجليزية من جانب مكينزي وميلنر (McKenzie and Milner)، تطورات الصين، مارس/ آذار2009: آخر التطورات في حماية البيانات، 9 مارس/ آذار2009 (ماريسون فورستر – Morrison Foerster) متوفر على: http://www.mofo.com/international/CN_en/news/15332.html

237 أنظر هانتون ووِيليامز (Hunton & Williams)، إنذار عميل Client Alert، يناير/ كانون الثاني 2010. متوفر على: http://www.hunton.com/files/News/4bfa5361-4d8f-4c7e-af03-75055a82202c/Presentation/NewsAttachment/7d2612ba-40d6-4884-83de-. أنظر أيضاً مكنزي بي، وملن رجي (McKenzie, P. and Milner, G.) خصوصية البيانات في الصين: مراحل تطور القانون الجنائي، 25 يناير/ كانون الثاني 2010 (ماريسون فوستر). متوفر على: http://www.mofo.com/data-privacy-in-china-civil-and-criminal-law-developments-01-25-2010/..

ظلت قوانين خصوصية البيانات في الصين على مدى السنوات الخمس الماضية فيما يطلق عليه فترة «الأقاليم المتحاربة»، حيث كانت الولايات المعنية هي الإقطاعيات الكثيرة الهائمة في متاهات البيروقراطية بجمهورية الصين الشعبية.[238]

18) جمهورية كوريا: قاعد الأسماء الحقيقية

في يوليو/ تموز من عام 2007، اعتمدت جمهورية كوريا قانون التحقق من الاسم الحقيقي، والذي ينص في نسخته الحالية على أن تقوم جميع المواقع التي تزيد حركة المرور اليومية فيها عن 100,000 زائر بتحديد هوية المستخدمين الذين يقومون بتحميل مواد أو نشر تعليقات باستخدام أسمائهم الحقيقية، ومن الناحية العملية في العادة من خلال استخدام أرقام تسجيل المقيم (RRN). ويهدف القانون إلى معالجة بعض المشاكل مثل العدد المتزايد من الاتهامات المغرضة والاحتيالية عبر الإنترنت والاعتداء على الخصوصية والاعتداء من خلال الإنترنت.

من الناحية الفنية، لا تشترط القواعد أن تقوم الشركات بإنشاء قواعد بيانات للمعلومات الشخصية، لأن لديها خيار مطالبة المستخدمين بالتزويد بالبيانات في كل مرة يقومون فيها بتسجيل الدخول. ولكن هذا غير عملي لأن معظم المستخدمين لن يكونوا على استعداد للقيام بذلك. ورفضت شركة جوجل (Google) الامتثال إلى ذلك، ومنعت المستخدمين من تحميل المحتوى على النسخة الكورية من متصفح يوتيوب (YouTube) على أساس أن قواعد التحقق من الاسم الحقيقي لا «تتماشى مع مبادئ جوجل (Google)». [239]

إن حادثة خرق البيانات الضخمة في يوليو/ تموز 2011 عندما قام قراصنة بسرقة المعلومات الشخصية لـ 35 مليون شخص كوري من شركة اتصالات كوريا الجنوبية (انظر المربع أعلاه) أدى إلى تجدد الدعوات لإلغاء هذا القانون، والذي أدى إلى تفاقم الآثار الناجمة عن تسرب البيانات. وفي أواخر شهر ديسمبر/ كانون الأول 2011، ذكرت الهيئة المعنية بتنظيم الإنترنت في البلاد، لجنة الاتصالات الكورية، بأنها ستنظر في القانون[240]، ولكن الإجماع على ما يبدو أنها من المرجح أن تلغيه.

238 أنظر جرينفيلد جي (Greenleaf, G.)، "خصوصية البيانات لآسيا والمحيط الهادي: 2011، عام الثورة؟" [2011] UNSWLRS 30، ص 5، متوفر على: http://law.bepress.com/unswwps/flrps11/art30/.

239 أنظر رويترز، نرفانا الإنترنت بكوريا الجنوبية تنفث نتائج جيدة وسيئة وقبيحة، 5 ديسمبر/ كانون الأول 2011. متوفر على http://www.msnbc.msn.com/id/45562846/ns/technology_and_science-tech_and_gadgets/t/south-koreas-net-nirvana-spawns-good-bad-ugly-results/#.Tw6t7Jj6QTM أنظر أيضاً http://www.zdnet.com/blog/foremski/google-refuses-compliance-with-korean-real-name-law-but-imposes-it-on-g-users/1920

240 أنظر http://www.hancinema.net/real-name-internet-law-on-way-out-36915.html

ثمة تطور كبير آخر تمثل في إصدار مشروع المبادئ التوجيهية لتقنية أمن المعلومات لحماية المعلومات الشخصية في فبراير/ شباط 2011، والصادر بالاشتراك بين وزارة الصناعة وتكنولوجيا المعلومات والإدارة الصينية للمقاييس (SAC) والإدارة العامة للرقابة على الجودة والتفتيش والحجز الصحي؛ وهي تشكل مجموعة غير ملزمة من قواعد حماية البيانات.

وتضع هذه المبادئ التوجيهية التي تنطبق على المعلومات المعالجة على الكمبيوتر تعريفاً واسع النطاق للمعلومات الشخصية على أنها أي معلومات يمكن استخدامها وحدها أو مع غيرها في تحديد هوية الفرد. ويشترط في غرض معالجة البيانات (وجمعها) أن يكون واضحاً ومعقولاً، ويشترط إخبار أصحاب البيانات بالغرض من معالجة البيانات والجهة القائمة بذلك، وكذلك حقوقهم (التي تتضمن حق الوصول إلى البيانات لتصحيحها والاعتراض على المعالجة الإضافية) وكيفية التقاضي. ولا يجوز معالجة البيانات إلا ما يتصل بالغرض المحدد منها. ويراعى سرية البيانات، ويجب أن تستخدم في الغرض المعلن فقط، ما لم ينص القانون أو يوافق صاحب البيانات على غرض آخر. وتنطبق قواعد خاصة على أنواع معينة من البيانات ذات الحساسية الخاصة. ويشترط موافقة ولي أمر من هم دون 16 سنة قبل أن يتم معالجة بياناتهم.

لهذه المبادئ التوجيهية قواعد صارمة بشأن نقل البيانات. حيث لا يجوز نقلها إلى الغير إلا بموافقة صاحبها، أو بنص قانوني أو تحت رقابة هيئة الرقابة. ولا يوجد أي استثناءات على هذه القواعد، على خلاف معظم الأنظمة الأخرى، مما يضفي عليها طابع الصرامة الشديدة، وربما تعذر تنفيذها.

وتتسم قواعد التحويلات الخارجية بصرامة أكبر، فلا يجوز التحويل الخارجي إلا بموجب القانون أو بإشراف هيئة الرقابة (حتى وإن تقدم صاحب المعلومات بتقديم الموافقة). ونظراً لانتفاء القوانين التي تنظم هذه التحويلات في الوقت الحالي (ربما مفهومة بسبب عدم ظهور هذه المسألة من قبل) وعدم وجود استثناءات عن الحاجة للحصول على إذن محدد (سواء بموجب القانون أو بإذن هيئة الرقابة)، فإن هذه القواعد تعتبر قيداً صارماً للغاية على تدفق البيانات عبر الحدود.

ونظراً لعدم إلزامية المبادئ التوجيهية، فإنه يمكن اختبارها على نطاق ضيق من حيث الواقع، ربما كتمهيد نحو اعتماد معايير واجبة النفاذ وفق القانون. ولهذا يعتبرها البعض غير عملية على صورتها الحالية.[241]

وتوفر مجموعة من الأحكام الواردة في القوانين والمبادئ التوجيهية الصينية المعتمدة منذ عام 2009 حماية البيانات الشخصية في قطاعات معينة مثل غسل الأموال والسجلات الطبية والتأمين وحماية المستهلك والتقارير الائتمانية.[242] كما كان هناك بعض التحرك التشريعي / التنظيمي على المستوى المحلي (المقاطعات والبلديات) لحماية الخصوصية، مثل قوانين حماية المستهلك وفيما يتعلق بالنظم الحاسوبية.[243]

---

241 أنظر مكنزي بي، وديكر إيه وفانج جي (McKenzie, P.; Dicker, A. and Fang, J.)، الصين تصدر مبادئ توجيهية جديدة بشأن حماية خصوصية البيانات، 11 إبريل 2011 (موريسون فوستر – Morrison Foerster) متوفر على: http://www.mofo.com/files/Uploads/Images/110411-China-Data-Privacy-Guidelines.pdf؛ فرنانديز (Fernández)، الصين تطبع مشروع المبادئ التوجيهية بشأن الخصوصية، 14 إبريل 2011 (هوجان لوفيلز – Hogan Lovells)، http://www.hldataprotection.com/2011/04/articles/international-eu-privacy/china-publishes-draft-privacy-guidelines/؛ روس إل، جاوي كي، وزاو إيه (Ross, L., Gao, K., and Zhou, A.) الصين تصدر مشروع مبادئ توجيهية بشأن الخصوصية على الإنترنت، تعلن وكالة جديدة لمراقبة الإنترنت، 19 مايو 2011 (ويلمر هالي – Wilmer Hale).

242 أنظر جرينليف (Greenleaf)، الحاشية 207، ص 7.

243 أنظر مكنزي و ميلنر (McKenzie and Milner)، الحاشية 236.

2.2.3. الهند

حتى وقت قريب، كان جنوب آسيا متأخرة بشكل كبير من حيث توفير الحماية للبيانات والخصوصية بشكل عام، مما دفع أحد الكتاب أن يصفها في العام 2009 باسم «الحد النهائي» لحماية البيانات في آسيا.[244] وبعد بضعة سنوات تغير الوضع على الأقل بشكل ملحوظ.

فلم يشتمل الدستور الهندي حقاً قائما بذاته بشأن الخصوصية. ومع ذلك، أورت المحكمة العليا الحق في الخصوصية كجزء من الحق في الحياة والحرية الوارد في المادة 21 التي تنص على ما يلي: "لا يجوز حرمان شخص من حياته أو حريته الشخصية إلا وفقا لإجراءات يقررها القانون.» وهكذا ذكرت المحكمة العليا في إحدى قضايا عام 1994 ما يلي:

> الحق في الخصوصية هو حق ضمني في الحق في الحياة والحرية المكفولة لمواطني هذا البلد بموجب المادة 21. وهو «الحق في أن يترك المرء وحده». وللمواطن الحق في حماية خصوصية شخصه وعائلته والزواج والأمومة والإنجاب والتعليم من بين أمور أخرى. ولا يجوز لأي شخص أن ينشر أي شيء بشأن المسائل المذكورة أعلاه دون موافقته. وإلا فإنه يعتبر بذلك منتهكاً للحق في الخصوصية للشخص المعني ويسأل عن أي أضرار.[245]

ولا يوجد حتى الآن قانون مدني مستقل بشأن الخصوصية في الهند، وإن كان هناك قانون تمت مناقشته لعدد من السنوات. ونتيجة لقضية عام 1994 المشار إليها أعلاه، كان على المحاكم إيجاد وسيلة انصاف لحالات الاعتداء على الخصوصية لأن المحكمة العليا رأت في هذه القضية أن نشر الأمور الخاصة «سواء كانت حقيقية أو غير حقيقية» يعتبر انتهاكا للحق في الخصوصية. وللقيام بذلك، ركزت المحاكم في الأساس على قواعد القانون العامة، مثل خرق الثقة.

وكان هناك مشروعاً شاملاً لقانون الخصوصية قيد المناقشة في الهند لبعض الوقت، رغم أنه في وقت كتابة هذا التقرير، لم يعتمد أي قانون. وتم تسريب مشروع قانون مؤرخ في 19 أبريل/ نيسان 2011 وبعنوان «مسودة العمل الثالثة (للمناقشة والتصحيح) القسم التشريعي" وهي الآن متوفرة على شبكة الإنترنت.[246] وكان هذا المشروع سيضع حقاً في الخصوصية قائما بذاته وشاملاً، بالإضافة إلى آلية قوية للتصدي لانتهاكات هذا الحق تسمى الهيئة العامة لحماية البيانات في الهند (DPAI).

وضع مشروع القانون تعريف واسع النطاق للخصوصية، حيث شمل أمور منها خصوصية الاتصالات والحياة الخاصة والعائلية والأعمال المصرفية والمعلومات الطبية وحماية البيانات والحماية ضد مختلف إجراءات الدولة مثل التفتيش والمراقبة. والجدير بالذكر أن القانون يقتصر في نطاقه على المواطنين الهنود فقط، ومن ثم فلا ينطبق على الأنشطة الخارجية. ويُستثنى من تطبيق القانون بعض الأنظمة القانونية القائمة، بما في ذلك تلك التي تتعلق بالحق في الحصول على المعلومات ومكافحة الفساد، ولكن يبدو أن مشروع القانون سوف يحتفظ بجميع القوانين القائمة من قبل في هذا المجال (انظر القسم 3).

كانت الهيئة العامة لحماية البيانات في الهند (DPAI) سيكون لها صلاحيات واسعة تشتمل على القيام بدور مسجل المتحكمين في البيانات للتحقيق في الانتهاكات، ومطالبة المتحكمين في البيانات باتخاذ إجراءات معينة

---

244 جرينليف جي (Greenleaf, G.,)، "واحد وعشرون سنة من حماية البيانات في أسيا والمحيط الهادي" (2009) 100 قانون لحماية الخصوصية ومقال إخباري دولي عن الأعمال 21.

245 آر راجاغوبال ضد ولاية تاميل نادو (R. Rajagopal v. State of Tamil Nadu) (1994) 6 SCC 632. هذه القضية أمدت الحق في الخصوصية بوضع التزام على الدولة لمنع التعدي على الحياة الخاصة. تم الاعتراف بالحق في المحكمة العليا في قضية جوفيند ضد ولاية مادهيا براديش و أنر (Govind v. State of Madhya Pradesh & Anr) (1975)، SCR (3) 946.

246 متوفر على: http://bourgeoisinspirations.files.wordpress.com/2010/03/draft_right-to-privacy.pdf.

لإنهاء أي انتهاكات، بالإضافة إلى صلاحية تلقي بعض الشكاوى (لم تحدد حتى الآن). وسيتمكن الأفراد أيضا من تقديم شكوى إلى محكمة استئناف اللوائح بقبرص، التي أنشئت بموجب المادة 48 من قانون تكنولوجيا المعلومات لسنة 2000،[247] والتي كان لها الصلاحية، من بين أمور أخرى، لفرض تعويضات عن الانتهاكات.[248] ولكن كما نلاحظ يظل هذا التشريع مجرد مشروع قانون خاضع للتغيير قبل أن يمرر ويصبح قانوناً.

تنص الكثير من القوانين الهندية على الحماية ضد الاعتداء على الخصوصية من قبل الدولة، مثلا في مجال تنفيذ القانون وإن كانت هناك بعض الاستثناءات، كما هو الحال في جميع البلدان. ومن ثم يشترط قانون العقوبات حصول الشرطة على إذن قبل إجراء التفتيش. وهذه القواعد خضعت للتعديل ضمن الفقه الدستوري للمحكمة العليا التي رأت على سبيل المثال أن التنصت على المكالمات الهاتفية يعتبر اعتداء على الخصوصية ومن ثم يتطلب تبريراً مقنعاً.[249]

الاتصالات السلكية واللاسلكية مكفولة بشكل عام عملاً بقانون المراسلات البرقية الهندي لسنة 1885،[250] وقانون تقنية المعلومات لسنة 2000. وقد أضاف القانون الأخير بعد تعديله جريمة جنائية محدودة لانتهاكات معينة للخصوصية على الإنترنت،[251] ونصت التعديلات التي أدخلت عليه في عام 2008 على اعتراض الاتصالات السلكية واللاسلكية عند الضرورة أو الحاجة لحماية السيادة أو السلامة أو الأمن في الهند، والعلاقات الودية مع الدول الأخرى، والنظام العام، ومنع التحريض على الجريمة أو تقويض التحقيقات في الجرائم.[252] كما إن هيئة تنظيم الاتصالات في الهند (TRAI)، التي أنشئت بموجب قانون هيئة تنظيم الاتصالات في الهند لسنة 1997،[253] لها صلاحيات واسعة في هذا المجال، وأصدرت أوامر قانونية مختلفة لحماية خصوصية الاتصالات.[254]

وتجدر الإشارة هنا إلى قانون الحق في المعلومات لسنة 2005،[255] الذي ينص على حق الحصول على جميع المعلومات التي تحتفظ بها السلطات العامة، باستثناء أي قانون آخر، وبالاستثناءات التي ينص عليها. وتنص المادة 8 (ي) من القانون على حماية الخصوصية على النحو التالي:

البيانات التي تتعلق بالمعلومات الشخصية والتي لا يتعلق الكشف عنها بأي نشاط أو مصلحة عامة، أو التي من شأنها أن تسبب تعدياً غير مبرر على خصوصية الفرد ما لم يقتنع مسؤول الإعلام المركزي أو موظف الإعلام العام بالدولة أو هيئة الاستئناف، حسب الحال، بأن هناك مصلحة عامة أكبر تبرر الكشف عن تلك المعلومات:

---

247 رقم 21 لسنة 2000.

248 لمزيد من المعلومات حول مشروع قانون الخصوصية أنظر جوبتا إيه (Gupta, A.)، "تحليل مشروع قانون الخصوصية، 2011" بشأن القانون الهندي ومدونة التكنولوجيا، 27 يونيو 2011 و جرينليف جي (Greenleaf, G.)، "منعطفات الهند بشأن خصوصية البيانات" سلسلة من أربعة أبحاث طبعت في (2011) 110–114 قوانين الخصوصية وتقرير الأعمال الدولي.

249 أنظر الاتحاد الشعبي للحريات المدنية ضد اتحاد الهند وآنر (People's Union for Civil Liberties (PUCL) v. Union of India and Anr). (1997) 1 SCC 301.

250 رقم 13 لسنة 1885، مثلا، القسمين 5 و 7.

251 أنظر القسم 66–E.

252 قانون تكنولوجيا المعلومات (وتعديلاته)، 2008، رقم 10 لسنة 2009، القسم 34، بتعديل القسم 69 من القانون الأصلي وإضافة القسم 69A والقسم 69B.

253 رقم 24 لسنة 1997

254 أنظر على سبيل المثال التوجيه الوارد ضمن القسم 13، البند الفرعي (1) من البند (ب) من القسم الفرعي (1) من القسم 11 من قانون هيئة تنظيم الاتصالات بالهند (24 لسنة 1997) لضمان الالتزام بشروط وأحكام الرخصة من جانب مزودي الخدمة فيما يتعلق بسرية معلومات المشتركين وخصوصية الاتصالات، 26 فبراير 2010.

255 رقم 22 لسنة 2005.

شريطة ألا يمنع أي شخص من الحصول على المعلومات التي لا يمكن حجبها عن البرلمان أو الهيئة التشريعية بالدولة.

وهذا يتضمن استثناء قوياً يتمثل في المصلحة العامة.

أخيراً وليس بآخر، في 11 أبريل/ نيسان 2011، اعتمدت وزارة الاتصالات وتكنولوجيا المعلومات بالهند قواعد تكنولوجيا المعلومات (الممارسات والإجراءات الأمنية المعقولة والبيانات أو المعلومات الشخصية الحساسة) لسنة 2011، عملا بالقسم 43A من قانون تقنية المعلومات لسنة 2000. وهذه القواعد هي عبارة عن نظام مصغر لحماية البيانات لا يختلف كثيراً عن معظم الأنظمة المماثلة في البلدان الأخرى. ومن المثير أنها تنطبق حصرا على القطاع الخاص، على خلاف معظم البلدان الأخرى التي تنطبق فيها هذه القواعد في المقام الأول على القطاع العام ثم قد تنطبق على القطاع الخاص.

ومن حيث الجوهر، تقتضي القواعد أن يقوم المتحكمون في البيانات بتطبيق سياسات حماية البيانات، والتي توضح ممارساتها وسياساتها، وتشير إلى نوع البيانات التي يتم جمعها وأغراض الجمع والغرض من الكشف عن المعلومات ووضع سياسة حماية أمنية لحماية تلك البيانات (القسم 4). وتقتصر معظم هذه القواعد من حيث النطاق على البيانات الشخصية الحساسة، مثل المعلومات الطبية أو المالية، ولكن أيضا تشتمل على معلومات تتعلق بالميول الجنسي. وتقتضي القواعد أيضا الإبلاغ المعقول عن جمع البيانات الشخصية والغرض من ذلك والمستلمين المقصودين. ولا يجوز أن تستخدم البيانات إلا للأغراض المذكورة، وهناك أيضا قواعد بشأن الحصول على البيانات وتصحيحها، وقواعد تتعلق بالأمن (المادة 5). إن الامتثال إلى المعيار IS/ISO/IEC 27001 حول "تقنية المعلومات – تقنيات الأمن – نظام إدارة أمن المعلومات – المتطلبات" يعتبر ضمانة كافية لأمن المعلومات (المادة 8).

وفي حين لم يقرر النطاق المحدد لهذه القواعد بعد، وبينما تظل محدودة مقارنة بالعديد من البلدان، إلا أنه في نفس الوقت يمكننا القول بأن اعتماد هذه القواعد قد كفل للهند مستوى جديد من حماية البيانات الشخصية.

3.2.3. مصر

لم تكن حماية الخصوصية من الأولويات في مصر على مر التاريخ. بل كانت قوات الأمن قادرة على الحصول على قدر كبير من المعلومات الشخصية، سواء عبر الإنترنت أو بدون الإنترنت، على الرغم من تنظيم ذلك بموجب قانون الإجراءات الجنائية. ولا يوجد قانون مكرس لحماية الخصوصية. ولكن ننتظر لنرى هل سيتغير ذلك مع الثورة والتغييرات الواسعة الديمقراطية التي نتجت عنها أم لا.

في وقت كتابة هذا التقرير، كان الدستور المصري هو عبارة عن الإعلان الدستوري الذي أصدره المجلس الأعلى للقوات المسلحة في 23 مارس/ آذار 2011، بعد استفتاء 19 مارس/ آذار 2011 على تسع مواد انتقالية. واحتوى الإعلان على 49 مادة، بالإضافة إلى هذه المواد التسع، جاءت من دستور 1971، بما في ذلك المادة 11 (حتى تاريخه)، التي تنص على ما يلي:

> لحياة المواطنين الخاصة حرمة يحميها القانون. وللمراسلات البريدية والبرقية والمحادثات التليفونية وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محددة ووفقا لأحكام القانون.

حتى وقت كتابة هذا التقرير، لم يكن هناك قانون شامل للخصوصية أو أي قانون لحماية البيانات. وتوجد قواعد الخصوصية في عدد من التشريعات القطاعية، ولكنها عادة ما تتناقض في طبيعتها. وخير مثال على ذلك قواعد الخصوصية في قانون تنظيم الاتصالات.[256] حيث نصت المادة 13 منه عند وصف دور الجهاز،

---

256 قانون تنظيم الاتصالات رقم 10 لسنة 2003.

أي الجهاز القومي لتنظيم الاتصالات (NTRA)، على أن يقوم بالمراقبة على تنفيذ تراخيص الاتصالات لضمان كفالة حقوق المستخدمين، "وخاصة حقوق الخصوصية».

ومع ذلك، تنص المادة 64 على أن يلتزم جميع مقدمي خدمات الاتصالات بتوفير الإمكانيات الفنية اللازمة التي "تتيح للقوات المسلحة وأجهزة الأمن القومي ممارسة اختصاصها في حدود القانون". وبشكل رسمي، يجب أن يتم ذلك مع "مراعاة حرمة الحياة الخاصة للمواطنين والتي يكفلها القانون"، ولكن عمومية المادة 64، فضلاً عن التركيز العام للإطار القانوني، تدل على تجاهل هذا من الناحية العملية في الماضي.

تنص المادة 58 من ذات القانون على أن يتولى الجهاز تجميع وإدارة وتحديث قاعدة بيانات مستخدمي الطيف الترددي، شريطة أن يلتزم الجهاز «بالحفاظ على سرية هذه البيانات حماية لحق المستخدمين في الخصوصية». وفي معظم الدول تكون هذه البيانات عامة على أساس أن الطيف الترددي هو مورد عام وأن للجميع الحق في معرفة المرخصين باستخدامه.

4.2.3. فرنسا

فرنسا هي من البلدان التي تفخر بتوفيرها ضمانات قوية لحماية الخصوصية. فبينما هناك دعم وطني قوي لهذا، تعرض النظام لتمحيص متزايد في أعقاب قضية ستراوس كان (Strauss-Kahn affair)، حيث اعتبر أن الحماية التي لا مبرر لها في فرنسا لحرمة حياة الأثرياء والمشاهير منعت وسائل الإعلام من الكشف عن الأفعال التي ارتكبها دومينيك شتراوس (Dominique Strauss-Kahn) والتي (يدعى أن) لها أهمية لكونها مخلة بالآداب.[257]

ومن المستغرب على الرغم من ذلك أن دستور عام 1958 لم ينص على حماية صريحة للخصوصية. ولكن في عام 1995 قضت المحكمة الدستورية أن الحق كان ضمنيا في الدستور،[258] وأكدت ذلك في قرار عام 1999.[259]

تنص المادة 9 من القانون المدني، والتي أضيفت في عام 1970،[260] على حماية الخصوصية حيث تشير ببساطة: "لكل شخص الحق في احترام حياته الخاصة." وتوضح الفقرة الثانية من هذه المادة أنه، بالإضافة إلى التعويض، يجوز للمحاكم الأمر «بفرض العزل والحجز وغير ذلك من الإجراءات المناسبة لمنع الاعتداء على الخصوصية ووضع حد له، وعلى أساس مؤقت في حالات الطوارئ. تطبق هذه القواعد من خلال المادة 1382 من القانون المدني، التي تنص على المبادئ العامة للمسؤولية عن الأضرار المدنية.

---

257 أنظر على سبيل المثال جوبنيك إيه، دي إس كي: الحياة الفرنسية، القوانين الفرنسية، 16 مايو 2001. متوفر على: http://www.newyorker.com/online/blogs/newsdesk/2011/05/dsk-french-lives-french-law.html

258 القرار رقم 94-352 DC بتاريخ 18 يناير/ كانون الثاني 1995، Recueil، ص 170 – الجريدة الرسمية بتاريخ 21 يناير/ كانون الثاني 1995، ص 1154. متوفر على: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1995/94-352-dc/decision-n-94-352-dc-du-18-janvier-1995.10612.html.

259 القرار رقم 99-416 DC بتاريخ 23 يوليو 1999، Recueil، ص 100– الجريدة الرسمية بتاريخ 28 يوليو 1999، ص 1125، متوفر على: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1999/99-416-dc/decision-n-99-416-dc-du-23-juillet-1999.11847.html. أنظر كذلك بالأخص الفقرة 45.

260 القانون رقم 70-643 بتاريخ 17 يوليو 1970.

من الناحية العملية، طبقت المحاكم الفرنسية هذه القواعد بصرامة، وفسرت بأن الحياة الخاصة تشمل، من بين أمور أخرى، علاقة الحب، والصداقات، والظروف الأسرية، والأنشطة الترفيهية، أو الآراء السياسية أو النقابية، أو الانتماء الديني، والحالة الصحية.[261]

وتطبق فرنسا كذلك أحكاما جنائية صارمة على الخصوصية في المواد 226–1 إلى 7 من قانون العقوبات. وتنص المادة 226–1، تعتبر جريمة يعاقب عليها بالسجن لمدة تصل إلى عام وغرامة تصل إلى 45000 يورو كل انتهاك عمد للحياة الخاصة للغير بدون موافقته عن طريق:

اعتراض أو تسجيل أو نقل كلمات قالها بثقة أو في ظروف خاصة؛

أخذ أو تسجيل أو نقل صورة الشخص في مكان خاص.

ولكن تفترض الموافقة عند تنفيذ هذه الإجراءات على مسمع ومرأى من الشخص دون اعتراضه مع تمكنه من الاعتراض. كل هذه الأحكام المقصورة على المناطق الخاصة والمحادثات السرية فهمها الجميع على أنها تستهدف في الأساس المصورين للشخصيات البارزة.

ركزت المادة 226–2 أكثر على وسائل الإعلام، وطبقت العقوبات نفسها على حفظ وإطلاع الجمهور العام أو استخدام أي وثائق بأي طريقة من الطرق أو تسجيلات تم الحصول عليها بما يخالف المادة 226–1. وتنص المادة 42 من قانون حرية الصحافة 29 يوليو/ تموز 1881 على أن من يتحمل المسؤولية عن هذه الجرائم عندما ترتكب في الصحافة هو مدير تحرير (رئيس التحرير). ووفقا للمادة 226–6، لا يجوز مباشرة هذه الإجراءات الجنائية إلا عند استلام شكوى من المجني عليه.

ويضمن القانون رقم 91–646 المؤرخ في 10 يوليو/ تموز 1991، والذي يحمل عنوان متصل بسرية المراسلات الصادرة عن طريق الاتصالات الإلكترونية، حماية سرية الاتصالات الالكترونية كما يوحي الاسم. وعملا بالمادة 3 يمكن اعتراض الاتصالات بإذن استثنائي لأغراض منها الحفاظ على الأمن ومكافحة الإرهاب أو الجريمة، أو لحماية مصالح اقتصادية أو علمية هامة للبلاد. وتنظم الإجراءات الصارمة التصريح بهذا الاعتراض وذلك وفقا للمادة 4 (ويمنح التصريح في النهاية من جانب رئيس الوزراء أو أحد المخولين الآخرين).

كما أن لفرنسا نظام قوي وقائم منذ أمد طويل لحماية البيانات الشخصية، مثل قانون عام 1978 لحماية البيانات.[262] حيث يطبق القانون بصيغته المعدلة توجيه الاتحاد الأوروبي لحماية البيانات بكل ما فيه من قواعد، بما في ذلك إنشاء "اللجنة الوطنية للمعلومات والحريات» (CNIL) كهيئة إدارية رقابية مستقلة. ومن المميزات التي يتسم بها القانون الفرنسي أنه يشترط على المتحكمين في البيانات تحديد فترة احتفاظ متوافقة مع الغرض المقصود (المادة 30 (1) (5)).

قد نفذت فرنسا أيضا توجيه الاتحاد الأوروبي للاحتفاظ بالبيانات، وطلبت من مقدمي خدمات الاتصالات الاحتفاظ ببيانات حركة المرور بين المواقع لمدة عام واحد. وهذا المطلب يواجه اعتراضاً أمام مجلس الدولة، وهو بمثابة المحكمة الإدارية العليا في فرنسا، من قبل حوالي 20 شركة تعمل على الإنترنت في فرنسا.[263]

ثم انتقلت فرنسا إلى تنفيذ توجيه الاتحاد الأوروبي رقم 2009/136، أو ما يعرف باسم «توجيه ملفات تعريف الارتباط". واعتمد مجلس الوزراء الفرنسي قراراً بتنفيذ التوجيه بتاريخ 24 أغسطس/ آب 2011. واستوجب

---

261 أنظر ambafrance-us.org/spip.php?article640

262 القانون رقم 78–17 لسنة 1978 بشأن معالجة البيانات، ملفات البيانات والحريات الفردية، وتعديلاته بالقانون رقم 2004–801 بتاريخ 6 أغسطس/ آب لسنة 2004 فيما يتعلق بحماية الأفراد بشأن معالجة البيانات الشخصية.

263 أنظر News Wires، كبرى شركات الإنترنت تعترض على قانون حماية البيانات الفرنسي بشأن الخصوصية، 6 إبريل 2011. متوفر على: http://www.france24.com/en/20110406-internet-giants-challenge-france-data-law-privacy-google-facebook-ebay. لا يمكن معرفة مرحلة هذه الإجراءات في الوقت الحالي.

التوجيه إخبار المستخدمين عن تثبيت واستخدام ملفات تعريف الارتباط، ويتم ذلك بموجب القواعد قبل تثبيت ملف تعريف الارتباط لأول مرة. ومع ذلك، تنص القواعد الفرنسية على أنه إذا تم ضبط المتصفحات بما يجعلها تقوم بتثبيت ملفات تعريف الارتباط، فإن الوضع الافتراضي في معظم أجهزة الكمبيوتر هو أنه ليس على المستخدمين تقديم موافقة صريحة.[264] ويبدو أن هذا هو بمثابة حل ينحرف تجاه مصالح مرضية، بدلا من تشكيل مسار خصوصية قوي، ويبقى أن نرى ما إذا كان سيعتبر مقبولا كوسيلة لتنفيذ التوجيه.

19) الضمانات الدستورية لحماية البيانات في أمريكا اللاتينية

من المزايا الفريدة نسبيا التي تمتاز بها بلدان أمريكا اللاتينية التواجد القوي للضمانات الدستورية الواضحة لحماية الحق المحدود في الحصول على المعلومات أمام المحكمة. وفي معظم البلدان الأخرى، تكون ضمانات الخصوصية عامة في طبيعتها ولكن وفقا لبعض التقديرات، يشتمل ثلثا دساتير أمريكا اللاتينية تقريبا على هذا النوع من الحماية الصريحة. ومن الأمثلة على ذلك:

المكسيك: تنص المادة 6 من الدستور على: «لكل فرد الحق في حماية بياناته الشخصية».

البرازيل: تنص المادة 5(0)(71) من الدستور على: «يمنح الحق في الحصول على البيانات أمام المحكمة:

لضمان معرفة المعلومات المتعلقة بشخص صاحب الالتماس، والواردة في السجلات أو بنوك البيانات لدى الجهات الحكومية أو الهيئات العامة؛

(أ) لتصحيح البيانات، إذا كان صاحب الالتماس غير راغباً في القيام بذلك من خلال الإجراءات السرية أو القضائية أو الإدارية؛

أوروغواي: تنص المادة 66 (19) من الدستور على: «الحقوق التالية للأشخاص معترف بها ومكفولة: الحق في حماية المعلومات الشخصية، بما في ذلك الحق في الحصول على المعلومات والبيانات من هذا النوع واتخاذ القرار بشأنها، فضلا عن حماية المراسلات. ويشترط في جمع هذه البيانات والمعلومات وحفظها ومعالجتها ونشرها وتوزيعها توافر الإذن من صاحبها أو صدور أمر قضائي.»

5.2.3. الأرجنتين

يشتمل دستور الأرجنتين على حق مستقل في الخصوصية، على غرار ما هو وارد في دساتير عديدة، فنصت المادة 19 منه على ما يلي:

> الأفعال الخاصة للأفراد التي لا تضر بأي حال من الأحوال بالنظام العام أو الآداب العامة، ولا تضر الغير، هي محفوظة فقط للرب وتُعفى من سلطة القضاة. ولا يلتزم أي فرد من الأمة بأداء ما لا يتطلبه القانون ولا يُحرم مما ليس محظور.[265]

وينص الدستور كذلك، تماشيا مع العديد من دساتير أمريكا اللاتينية، على الحق في الحصول على البيانات أمام المحكمة في المادة 43 على النحو التالي:

264 أنظر http://www.privacysecuritysource.com/2011/09/09/france-implements-the-cookies-directive-and-strengthens-its-privacy-laws/

265 أنظر أيضاً قضية Ponzetti de Balbín، الحاشية 128.

يرفع كل شخص هذه الدعوى للمطالبة بالحصول على معلومات تتصل بما له من بيانات والغرض منها، والمسجلة في السجلات العامة أو قواعد البيانات، أو المسجلة في السجلات الخاصة المعدة للتزويد بالمعلومات؛ وفي حال وجود بيانات غير صحيحة أو التعرض للتمييز، يجوز رفع الدعوى بطلب حجز أو تصحيح أو الاحتفاظ بسرية أو تحديث تلك البيانات. لا يجوز المساس بالطبيعة السرية لمصادر المعلومات الصحفية.

ويكفل القانون المدني كذلك حماية الخصوصية، حيث تنص 1071 مكرر،[266] على نطاق واسع من حماية الخصوصية، ولم تعتبرها فعل إجرامي. وفي حالة خرق الحق في الخصوصية، تأمر المحكمة بوقف العملي المتعدي على الخصوصية إذا لم يحدث ذلك من قبل، وربما تأمر بدفع تعويضات. ويجوز للمحكمة أن تأمر بنشر الحكم في صحيفة أو مجلة إذا رأت في ذلك إنصافاً. وهذه المادة تنطبق بشكل كبير في الأرجنتين لحماية أنواع مختلفة من مصالح الخصوصية.

وفي سلسلة من القضايا، أصدرت المحاكم في الأرجنتين أوامر أولية ضد محركات البحث التي تديرها شركتي جوجل (Google) وياهو (Yahoo).[267] وفي جميع هذه الحالات تم نشر البيانات الشخصية للمدعي (الذي كان دوماً من المشاهير أو الشخصيات المعروفة)، مثل اسمه أو صورة له، على مواقع طرف ثالث دون موافقته، وعادة لترويج بيع محتوى أو خدمات جنسية. وبدلا من مقاضاة المسؤولين مباشرة، يلجأ المدعون إلى مقاضاة محركات البحث، وذلك ربما على أمل منع الوصول إلى هذه المعلومات بطريقة أكثر منهجية.

وكان يصدر في كثير من الحالات الأوامر الأولية ضد محركات البحث على أساس مشاركتها في تفاقم هذا الخرق لحقوق الخصوصية للمدعين. وصدرت الأوامر في كثير من الأحيان ليس لقطع الروابط المتصلة بالمواقع الواردة في الدعوى فقط، ولكن أيضاً المتصلة بمواقع أخرى مماثلة. ولا يعتبر هذا بالأمر الصعب للغاية من الناحية الفنية، بل هو بمثابة انتهاك للقانون الدولي.[268]

ويبقى من غير الواضح مدى تأثير ذلك في نهاية الأمر، رغم إلغاء بعض القرارات الأولية. وبالتالي، في قضية فيرجينيا دو كونها ضد ياهو دو أرجنتينا واي أوترا (Virginia da Cunha c/ Yahoo de Argentina y Otro)[269] تقرر التعويض بمبلغ 50.000 بيزو أرجنتيني (ما يقارب 12.000 دولار أمريكي) في حق كل من جوجل (Google) وياهو (Yahoo). ومع ذلك، في أغسطس/ آب 2010، ألغي القرار بالقرار رقم 2-1 عن محكمة الاستئناف.[270]

---

266 مضاف بالمادة 1 من القانون رقم 21.173، منشور في الجريدة الرسمية بتاريخ 22 أكتوبر/ تشرين الأول 1975.

267 تأتي معظم المعلومات عن هذه القضايا من كومبا إي، وبيرتوني إي (Compa, E. and Bertoni, E.,) الأنماط الناشئة في حرية التعبير على الإنترنت: نتائج بحث مقارن في الأرجنتين وخارجها (مركز دراسات حرية التعبير والحصول على المعلومات) (CELE). متوفر على: http://www.palermo.edu/cele/libertad-de-expresion-en-Internet.pdf.

268 أنظر على سبيل المثال الإعلان المشترك لعام 2011 بشأن الإنترنت وحرية التعبير للولايات الأربع الدولية الخاصة بشأن حرية التعبير، متوفر على: http://www.law-democracy.org/wp-content/uploads/2010/07/11.06.Joint-Declaration.Internet.pdf.

269 Da Cunha Virginia c/ Yahoo de Argentina SRL y otro s/ Daños y perjuicios Juz. Nac. En lo Civil nø 75, Expte. Nø 99.620 06/29 يوليو2009 .

270 أنظر http://www.nytimes.com/2010/08/20/technology/internet/20google.html

وينص قانون العقوبات الأرجنتيني، وتعديلاته بموجب القانون رقم 26.388 بشأن انتهاكات الاتصالات الإلكترونية وغيرها من الأعراف [271]، على عقوبات على جرائم تقنية المعلومات المختلفة. وأعيد تسمية القانون ليصبح الباب الخامس من الفصل الثالث من قانون العقوبات «كـانتهاك السريات والخصوصيات". وتعتبر المادة 153 التي تتناول انتهاكات الاتصالات الإلكترونية أن الوصول إلى أي مراسلات الكترونية أو خطابات أو فاكسات أو برقيات والحصول عليها دون موافقة يعتبر جريمة. وتعتبر كذلك جريمة قيام أي شخص غير مصرح له بحذف أو تحويل أي مراسلات إلكترونية، أو اعتراضها أو تسجيلها، وكذلك الوصول غير المصرح به إلى قواعد البيانات الخاصة أو العامة ونظم تكنولوجيا المعلومات وتوفير معلومات منها إلى أطراف ثالثة.

كانت الأرجنتين واحدة من أوائل الدول في أمريكا اللاتينية التي اعتمدت قانون حماية البيانات في صورة قانون حماية البيانات الشخصية لسنة 2000.[272] إن كون القانون يكفل حماية قوية للبيانات الشخصية قد ينظر إليه من حيث انفراد الأرجنتين بالاعتماد من المفوضية الأوروبية كالدولة الوحيدة في أمريكا اللاتينية التي كفلت مستوى كاف من الحماية للبيانات الشخصية.[273] ويبدو أن القانون مستمد من المعايير الأوروبية لحماية البيانات.[274]

6.2.3. المكسيك

يكفل الدستور المكسيكي حماية واسعة النطاق للخصوصية في المادة 16، التي تنص في الجزء ذي الصلة على ما يلي:

> لا يجوز إزعاج أي شخص في حياته الشخصية أو العائلية أو في مسكنه أو أوراقه أو ممتلكاته إلا بأمر كتابي عن جهة مختصة على أساس قانوني وأسباب إجرائية قانونية.
>
> تصدر جميع أوامر التفتيش محدد فيها مكان التفتيش والشخص أو الأشخاص المقرر ضبطهم والأشياء المقرر البحث عنها، ولا تصدر هذه الأوامر إلا عن السلطة القضائية المختصة بالتنفيذ ويتشرط أن تصدر كتابة. ويلزم مراعاة تنفيذ التفتيش كإجراء مقيد، في حضور اثنين من الشهود يحددهم قاطن المكان؛ وفي حال عدم وجودهم أو رفضهم للحضور، تلتزم السلطات المعنية بالتفتيش بالرعاية والاهتمام.
>
> الاتصالات الخاصة مصونة: يجرم القانون أي فعل يرتكب ضد حرية الاتصالات أو خصوصيتها. ولا يجوز لأي أحد أن يصرح باعتراض الاتصالات الخاصة إلا السلطة القضائية الاتحادية بناء على طلب موجه إلى السلطة الاتحادية المعنية بتنفيذ القانون أو لرئيس النيابة العامة الاتحادية للهيئة الفيدرالية المعنية. ولهذا يجب أن تحدد السلطة المختصة كتابة وتبرر الأسباب القانونية للتطبيق، مع ذكر نوع الاعتراض والمقرر اعتراضهم ومدة الاعتراض. ولا يجوز للسلطة القضائية الاتحادية منح هذه التراخيص في المسائل الانتخابية أو التجارية أو المالية أو العمالية أو الإدارية، أو في حالة اتصالات متهم بمحاميه أو المدافع عنها.

---

271 نشر في الجريدة الرسمية بتاريخ 25 يونيو 2008.

272 القانون رقم 25.326، الصادر في 30 أكتوبر/ تشرين الأول 2000.

273 أنظر http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

274 في الدراسة الاستقصائية التي أجراها جرينفيلد (Greenleaf) قام بتقييم القانون الأرجنتيني على أنه يتميز بتسعة من بين عشرة مزايا من النظام الأوروبي التي يفتقد إليها نظام منظمة التعاون الاقتصادي والتنمية، الحاشية 207، ص 10.

يكون الاعتراض بما يتوافق مع شروط وحدود يقررها القوانين. وأي نتيجة يتوصل إليها الاعتراض غير المتوافق مع هذه الشروط والحدود لن يعتد بها في التحقيق.

يجوز للسلطة الإدارية زيارة المساكن فقط للتأكد من توافقها مع الأنظمة الصحية وأنظمة الشرطة، وطلب إظهار الكتب والأوراق التي لا غنى عنها للتحقق من اهتمام السكان بالترتيبات المالية مع مراعاة القوانين ذات الصلة والإجراءات المقررة في عمليات التفتيش.

يجب أن لا تخضع المراسلات عن طريق البريد إلى أي فحص، والإخلال بذلك جريمة يعاقب عليها القانون.

وبهذا يكفل الدستور حماية قوية للخصوصية بشكل عام ضد عمليات التفتيش وسرية الاتصالات.

وينص القانون المدني الاتحادي على توفير حماية مدنية للحق في الخصوصية، وكفل على وجه التحديد توفير سبل انصاف من الأضرار المعنوية التي تلحق بالفرد نتيجة لأعمال غير قانونية تمس «بمشاعره، أو عاطفته، أو معتقداته، أو لياقته أو شرفه أو سمعته، أو حياته الخاصة، أو التكوين أو الجوانب المادية له، أو رؤية الآخرين له». ويجوز التقاضي في حال مخالفة أي من هذه الأحكام.[275]

ومنذ عام 2002، كان هناك حماية للبيانات الشخصية التي تحتفظ بها السلطات العامة الاتحادية بموجب قانون الشفافية الاتحادي والوصول إلى المعلومات العامة الحكومية،[276] وهو القانون المكسيكي للحق في المعلومات أو حرية المعلومات. وعلى الرغم من أنه قانون يتعلق بالحق في المعلومات، إلا أن من بين أغراضه «ضمان حماية المعلومات الشخصية التي يمتلكها أفراد بموجب القانون» (المادة 4 (3)). ويضع الفصل الرابع من القانون نظاما لحماية البيانات الشخصية للحصول على معلومات، والذي يتضمن بعض القواعد مثل استخدام البيانات الشخصية في الأغراض التي جمعت من أجلها فقط، وضمان أمن هذه البيانات، ووضع سياسة استخدام البيانات، والاحتفاظ بالبيانات حديثة ودقيقة، وعدم الكشف عنها لأطراف ثالثة (إلا في ظروف معينة)، وإبلاغ الهيئة الرقابية بجمع البيانات الشخصية، وتوفير فرص الحصول على البيانات الشخصية وتصحيحها من جانب صاحبها. ويتولى الرقابة المعهد الاتحادي للوصول إلى المعلومات (IFAI)، (وهو المعهد الاتحادي للوصول إلى المعلومات وحماية البيانات حالياً).

ويقتصر نطاق قانون الحق في المعلومات بشكل كبير على الهيئات العامة الاتحادية. ومع ذلك، تم اعتماد قانون حماية البيانات العامة في عام 2010 ليكون ملزماً على الهيئات الخاصة في صورة قانون اتحادي لحماية البيانات الشخصية التي تحتفظ بها أطراف من القطاع الخاص. ويذكر جرينليف (Greenleaf) أن هذا القانون يتفق مع خمسة من بين المبادئ العشرة الرئيسية الأوروبية لحماية البيانات، ولم يشتمل على ما يلي:

- اقتصار جمع البيانات على ما هو ضروري لأغراض معلنة؛
- شرط إخطار جهاز حماية البيانات عند جمعها؛
- الالتزام بسرية هوية البيانات أو إتلافها بعد فترة معينة؛
- قيود على المعالجة الآلية للبيانات؛

---

275 أنظر على سبيل المثال سوليس ضد رايدومفيل ديسبا سا دو سي في (Solís v Radiomovil Dipsa SA de CV) (القضية رقم 642/99)، مقتبسه في شميدت إل و أرسيو إيه (Schmidt, L. and Arceo, A.) "حقوق السمعة والشهرة في المكسيك" في استعراض العلامة التجارية العالمية، سبتمبر(أيلول) / أكتوبر (تشرين الأول) 2008.

276 متوفر على: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB68/laweng.pdf. متوفر باللغة الاسبانية، وتعديلاته على: http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf

- شرط توفير حرية الاختيار بشأن استخدامات التسويق المباشر للبيانات.[277]

وفي الوقت نفسه، يجسد القانون معظم المبادئ الأساسية لحماية البيانات الموجودة في الأنظمة الأخرى.[278] ويتولى الرقابة كذلك المعهد الاتحادي للوصول إلى المعلومات (IFAI).

7.2.3. الولايات المتحدة الأمريكية

لعبت الولايات المتحدة الأمريكية دوراً حاسماً في مسائل الخصوصية على الصعيد العالمي ليس فقط بسبب وزنها ومكانتها الدولية، ولكن أيضا نظراً لهيمنتها الواسعة المتمثلة في الشركات التي تقدم خدمات الإنترنت. في الواقع، تتخذ معظم شركات التزويد بخدمات الإنترنت التي أصبح لها نفوذ عالمي من الولايات المتحدة مقراً لها – مثل جوجل (Google)، الفيسبوك (Facebook)، ياهو! (Yahoo!)، يوتيوب (YouTube)، تويتر (Twitter)، وويكيبيديا (Wikipedia).

للولايات المتحدة الأمريكية تاريخ طويل وقوي في مضمار توفير الحماية للخصوصية، وتميزت بالمبادرات التشريعية والمبتكرة في كثير من الأحيان. ولها في ذلك أيضاً تصور قوي جدا يقوم على حرية التعبير، بما فيها حرية التعبير التجارية، والتي اقترنت كثيرا بدعاوي الخصوصية في كثير من القضايا. علاوة على ذلك، أظهر المشرعون إحجاماً عن سن تشريعات مكرسة لقضايا الخصوصية على الإنترنت خشية تقويض النشاط الهائل للتجارة عبر الإنترنت و / أو خلق نظام رقابي غير قابل للتطبيق، مما أدى إلى وضع إطار قانوني شامل مثير للاهتمام يعتبر في بعض المجالات ميزة عالمية، بينما في مجالات أخرى، وعلى الأخص في مجال حماية البيانات، ليس كذلك على الإطلاق.

ليس ثمة ضمان مباشر للخصوصية في دستور الولايات المتحدة، على الرغم من استمداد حق محدود من عدد من الأحكام الدستورية الأخرى، وأهمها ما تم أخذه من التعديل الرابع – الذي يحمي من عمليات التفتيش والضبط غير المعقولة – حق الخصوصية ضد الولاية لدى المحكمة العليا في الولايات المتحدة في قضية كاتز ضد الولايات المتحدة (Katz v. United States) سنة 1967.[279] والمفهوم الأساسي هنا هو فكرة وجودة منطقة يتوقع فيها الأفراد وجود خصوصية تضم العناصر الشخصية (أي التوقع الفعلي) والموضوعية (أي التوقع المعقول). وكون هذا الجانب من الحق مستمد من التعديل الرابع يمنع أن يمتد، على غرار المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان، لينطبق على الجهات الخاصة. وقد كان هناك كم هائل من الرأي الفقهي بشأن هذه القواعد. وفي قضية أخيرة، حكمت المحكمة العليا بالولايات المتحدة أن توصيل جهاز تحديد المواقع العالمي (GPS) بإحدى السيارات يعد تفتيشاً، ومن ثم يندرج ضمن القواعد المتعلقة بالتفتيش (أي التي تتطلب أمر تفتيش في العادة).[280]

---

277 الحاشية 207، ص. 11.

278 أنظر على سبيل المثال أورانتيس جي، وكروز سي، وموررالز بي (.Orantes, J., Cruz, C. and Morales, P) "تطور قانوني": مرسوم بقانون اتحادي لحماية البيانات الشخصية في حيازة الشخص، وتعديل الفقرات الثانية والسابعة من المادة 3، والمادة 33 وعنوان الفصل الثاني من الباب الثاني من القانون الاتحادي للشفافية والوصول إلى المعلومات الحكومية العامة، متوفر على: /http://www.theworldlawgroup.com/files/file Mexico/docs%20DP.pdf، وبلاكمير إس (.Blackmer, S)، "قانون حماية البيانات المكسيكي الجديد"، 28 يوليو 2010، متوفر على: /http://www.infolawgroup.com/2010/07/articles/data-privacy-law-or-regulation /mexicos-new-data-protection-law.

279 389 الولايات المتحدة 347 (1967).

280 الولايات المتحدة ضد جونز (United States v. Jones)، رقم 10-1259، 23 يناير/ كانون الثاني 2012.

وقد اعتراف القانون لأكثر من قرن بالضرر الناتج عن انتهاك الخصوصية، والذي يمنح الحق في مقاضاة الجهات الخاصة والعامة، وهو الآن معترف به في كل ولاية تقريبا. وثمة أربعة إجراءات قانونية مكفولة بشأن الخصوصية بشكل عام، ومنها التدخل غير المعقول في عزلة الفرد، واستغلال الاسم أو الشبه، والدعاية التي تروج للفرد شهرة كاذبة والدعاية غير المعقول لحياة المرء الخاصة.[281]

ويضع قانون الخصوصية لسنة 1974 نظاماً لحماية البيانات، ولكن ينحصر على السلطات العامة فقط. أما الهيئات الخاصة فلها في معظم الأحيان حرية وضع معايير الخصوصية الخاصة بها.[282] وفي كثير من النواحي تتشابه قيم ومبادئ حماية البيانات الأساسية التي يقوم عليها قانون الخصوصية لتلك التي تضمنها توجيه الاتحاد الأوروبي لحماية البيانات، وإن اختلفت في نطاق التطبيق.[283] وفي نفس الوقت، تختلف الترتيبات المؤسسية اختلافاً كبيراً. ومن ثم فليس هناك هيئة رقابية مستقلة لحماية البيانات، كما هو مطلوب في توجيه الاتحاد الأوروبي. ولكن بدلا من ذلك يوجد مكتب الإدارة والموازنة (OMB) الذي يلعب دوراً محدوداً أكثر بشأن سياسة حماية الخصوصية.

بالإضافة إلى هذين النظامين المركزيين بشأن الخصوصية، هناك عدد كبير من البرامج النظامية في الولايات المتحدة الأمريكية التي تركز على مختلف القطاعات والمجالات المثيرة للقلق. ينص قانون خصوصية الاتصالات الإلكترونية لسنة 1986(ECPA)، والذي طبق أساسا تشريعات التنصت التقليدية في عصر الإنترنت، على الحماية للاتصالات الإلكترونية. وينقسم إلى ثلاثة أجزاء أو أبواب، وهي قانون التنصت، وقانون الاتصالات المخزنة، وقانون سجل أرقام الاتصال. وبشكل عام، يضمن الباب الأول سرية الاتصالات أثناء نقلها، ويضمن الباب الثاني، كما يوحي الاسم، سرية الاتصالات المخزنة، ويحظر الثالث من تعقب الرسائل الواردة والصادرة. ويمكن تجاوز الأبواب الثلاثة لأسباب مختلفة، وينص الأول على الحماية الأقوى للسرية. وقد أضعف قانون الأمن الوطني لسنة 2002 (أو قانون باتريوت كما يعرف) من حماية الخصوصية في قانون خصوصية الاتصالات الإلكترونية، ولا سيما من خلال توسيع صلاحيات الاعتراض لأغراض الأمن وتنفيذ القانون.

يسهل قانون جرام – ليتش – بلايلي (Gramm–Leach–Bliley Act) لسنة 1999 من تبادل المعلومات على نحو فعال بين المؤسسات المالية، مع وضع معايير خاصة لضمان الحماية المناسبة للخصوصية.[284] اعتمد في عام 1994 قانون حماية خصوصية السائق استجابة لبيع سجلات السيارات، بما فيها الكثير من البيانات الشخصية الحساسة – مثل أرقام الهواتف والعناوين والتفاصيل الشخصية والمعلومات الطبية – التي أدت إلى عدد من الجرائم الخطيرة كان من بينها قتل إحدى الممثلات الشهيرات. ويجرم قانون سجلات التلفون وحماية الخصوصية لسنة 2006 استخدام ذريعة كاذبة للحصول على أو شراء أو بيع السجلات الهاتفية الشخصية، في حين أنشأ قانون المعاملات الائتمانية العادلة والدقيقة لسنة 2003 بعض حقوق الخصوصية الجديدة، مثل الحق في الحصول على تقرير ائتمان مجاني من مكاتب الائتمان مرة في السنة. وكان جزءا من إستراتيجية شاملة لمواجهة انتحال الهوية.[285] ويشترط قانون حماية خصوصية الأطفال على الإنترنت لسنة 2000

---

281 انظر ليك ضد وال مارت ستور إنك (Lake v. Wal–Mart–Stores Inc.)، 30 يوليو 1998، محكمة مينيسوتا العليا، C7–97–263، أنظر أيضاً إعادة بيان الأضرار، § 1977) ،E–652B).

282 تداعيات أضرار الخصوصية على حماية البيانات كانت محدودة. أنظر تأثير معايير خصوصية البيانات الأوروبية خارج أوروبا: التداعيات لعولمة اتفاقية 108، الحاشية 207، ص. 5.

283 بيان مكتوب للبروفيسور بطرس بي واير موريتز (Professor Peter P. Swire Moritz) كلية القانون بجامعة أوهايو، مركز التقدم الأمريكي، مقدم إلى لجنة الطاقة والتجارة التابعة لمجلس النواب، 15 سبتمبر/ أيلول 2011، «الخصوصية على الإنترنت: تأثير وعبء تنظيم الاتحاد الأوروبي» متوفر على: http://www.americanprogressaction.org/issues/2011/09/pdf/swire_testimony.pdf.

284 مركز معلومات الخصوصية الالكترونية ومنظمة الخصوصية الدولية يصفا هذا «بالوهن». الحاشية 119، ص 1009.

285 أنظر: http://www.money-zine.com/Financial-Planning/Debt-Consolidation/Identity-Theft-Regulations/

(COPPA) موافقة أولياء الأمور قبل جمع المعلومات عن الأطفال دون سن 13 سنة. ويشترط كذلك قيام المواقع بوضع سياسات خصوصية، ومن ثم العمل على أساس نهج يقوم على التنظيم الذاتي.

وجاء قانون ضبط هجوم الصور الإباحية وإعلانات التسويق المتطفّلة لسنة 2004 (CAN–SPAM Act) كمحاولة لوضع معايير للرسائل غير المرغوبة، على الرغم من أنه يعتبر ذو تأثير قليل جداً. فهو لا يتطلب موافقة المتلقي للرسالة غير المرغوبة، ولكنه يتطلب قيام المرسل بالإشارة إلى أن هذه الرسالة هي إعلان وتزويد عنوان بريدي صالح للمرسل. وللمستلمين الحق في عدم تلقي الرسالة من خلال إرسال إشعار بذلك.

حتى الآن رفضت الولايات المتحدة الأمريكية اعتماد قواعد الاحتفاظ بالبيانات على غرار تلك المنصوص عليها في توجيه الاحتفاظ بالبيانات للاتحاد الأوروبي. وقد اقترحت مشاريع قوانين في هذا الصدد، مثل مشروع قانون منع الإنترنت من تسهيل استغلال البالغين لشباب اليوم لسنة 2009 (SAFETY Bill)، الذي اقترح في عام 2009 ولم يعتمد بها. حيث كان سيتطلب من مقدمي خدمات الاتصالات الاحتفاظ لمدة لا تقل عن سنتين "بكافة السجلات أو المعلومات الأخرى المتعلقة بهوية أي مستخدم لعنوان شبكة تخصصه الخدمة له بصورة مؤقتة.»[286]

بالإضافة إلى هذه القوانين الاتحادية، بذل الكثير من الجهد على مستوى الولايات للتركيز على مسألة الخصوصية والإنترنت.[287]

8.2.3. نيجيريا

تنص المادة 37 من دستور عام 1999 لجمهورية نيجيريا الاتحادية على ما يلي: « خصوصية المواطنين ومنازلهم ومراسلاتهم ومكالماتهم الهاتفية واتصالاتهم البرقية مكفولة بموجب هذه الدستور». ولكن تنص المادة 45 على أن هذا لا يبطل أي قانون «مبرر بشكل معقول في مجتمع ديمقراطي (أ) في مصلحة الدفاع، أو الأمن العام، أو النظام العام، أو الآداب العامة، أو الصحة العامة؛ أو (ب) لغرض حماية حقوق وحرية الآخرين». ولم يهتم الفقه الدستوري كثيراً بهذه القضايا، والتي يمكن أن توفر توجيهات بشأن نطاق هذه القيود من حيث التطبيق العملي.

لا توجد حماية صريحة للاعتداءات على الخصوصية في القانون المدني النيجيري، ولكن يفترض أن ينطبق إجراء الانصاف من خرق الثقة المنصوص عليه في القانون العام في نيجيريا، وبالتالي قد يعول عليه في الحماية المدنية.[288] ولكن، مثلما هو الحال في شأن الضمان الدستوري، لم يكن هناك أي دراسة فقهية محلية تذكر لهذه المسألة.

في الوقت الحالي، لا يوجد في نيجيريا أي قانون ينظم بالتحديد اعتراض الاتصالات الخاصة. ويوجد أمام البرلمان مشروعان لقانونين بشأن هذه المسألة، وهما مشروع قانون الاعتراض والمراقبة لسنة 2009، ومشروع قانون تسهيلات الاتصالات (الاعتراض المشروع للمعلومات) لسنة 2010.[289] وفقا لقانون الاتصالات النيجيرية لسنة 2003،[290] يفترض أن تعتبر الاتصالات خاصة، ورغم ذلك ينص القانون على اعتراض

---

286 http://www.wired.com/threatlevel/2009/02/feds-propose-st/

287 بعض هذه الجهود مذكور في: http://www.ncsl.org/default.aspx?tabid=13463

288 أنظر نواش، إي إس (Nwauche, E.S.)، "الحق في الخصوصية في نيجيريا" (2007) 1 مراجعة القانون والممارسة النيجيرية 63.

289 لمزيد من المعلومات عن هذين المشروعين يرجى الرجوع إلى أودو أودوما و بيلو أوساجي (Udo Udoma & Belo-Osagie)، القانوي: اعتراض الاتصالات الخاصة في نيجيريا، 7 مارس/ آذار2012. متوفر على: http://www.proshareng.com/articles/2406.

290 متوفر على http://www.nigeria-law.org/Nigerian%20Communications%20Commission%20Act%202003.htm

الاتصالات. حيث تنص المادة 147 منه على ما يلي: «يجوز للجنة أن تقرر بأن المرخص له أو فئة من المرخصين لهم يلتزمون بتنفيذ قدرة تسمح بالاعتراض المصرح به للاتصالات ويجوز لهذا التقرير أن يحدد المتطلبات الفنية لقدرة الاعتراض المصرح به». وتنص كذلك المادة 148 على اعتراض الاتصالات في حالة الطوارئ العامة.

وطُرح للمناقشة مشروعان آخران لقانونين يتعلقان على وجه التحديد بحماية المعلومات على أجهزة الكمبيوتر والإنترنت، وهما مشروع قانون أمن الكمبيوتر وحماية البنية التحتية الحيوية للمعلومات لسنة 2005 ومشروع قانون الأمن لالكتروني ووكالة حماية المعلومات لسنة 2008. وتحظر المادة 13 من المشروع الأول أي اعتراض غير قانوني لأي اتصالات، ولكنه يكفل صلاحيات واسعة للاعتراضات القانونية، منها على سبيل المثال لأغراض الكشف عن الجريمة ومنع وقوعها. ويحظر المشروع الثاني من الاعتراض غير المشروع، ولكنه يتطلب من مزودي خدمات الإنترنت أن تكون لديهم القدرة على اعترض الاتصالات لأغراض مساعدة أجهزة تنفيذ القانون (المادتان 16–17).[291]

لا يتضمن القانون النيجيري أي نظام شامل لحماية البيانات. وتنص المادة 12 (4) من مشروع أمن الكمبيوتر وحماية البنية التحتية الحيوية للمعلومات لسنة 2005 على شكل محدود جداً من حماية البيانات على النحو التالي:

> لا يجوز استخدام أي بيانات تم الاحتفاظ بها أو معالجتها أو استرجاعها من قبل مزود الخدمة بناء على طلب أي جهاز من أجهزة تنفيذ القانون بموجب هذا القانون أو بموجب أي تنظيم في هذه المادة، إلا لأغراض مشروعة. ولا يكون الغرض مشروعاً بموجب هذا القانون عند الاحتفاظ بالبيانات أو معالجتها أو استرجاعها إلا بموافقة من تخصهم البيانات أو بموجب أمر قضائي من المحكمة المختصة أو أي سلطة قضائية أخرى.

9.2.3. جنوب أفريقيا

مع انصرام حقبة الفصل العنصري (الأبارثيد) في جنوب أفريقيا، واجهت البلاد تحديا هائلا في بناء إطارها قانونية، بل واجتماعي وسياسي واقتصادي لتقوم عليه الديمقراطية. وأشار بعض المراقبين إلى أنه نظراً إلى السياق التاريخي الخاص، تركزت طاقات جنوب أفريقيا أكثر على حقوق المساواة، وذلك على حساب حقوق أخرى مثل الخصوصية. ومن الناحية القانونية، ثمة مبرر لذلك وهو أن البلاد حتى الآن لم تضع قانوناً لحماية البيانات، وإن وجد عدد من المصادر القانونية لحماية الخصوصية.

ينص دستور جمهورية جنوب أفريقيا 1996 على حماية الخصوصية في المادة 14 على النحو التالي:

لكل فرد الحق في الخصوصية، والذي يتضمن الحق فيما يلي:

(أ) عدم تعرض شخصه أو منزله للتفتيش؛

(ب) عدم تعرض ممتلكاته للتفتيش؛

(ج) عدم الحجز على ممتلكاته؛

(د) و عدم انتهاك خصوصية الاتصالات الخاصة به.

---

291 لمزيد من المعلومات حول هذين المشروعين، أنظر أكينسوي (Akinsuyi)، جريمة الإنترنت وتشريعات الخصوصية في نيجيريا، وقت المراجعة، 9 أغسطس/ آب 2010. متوفر على: file:///Users/toby/Documents/ 20law.webarchive%20Crime%20UNESCO/Country/Nigeria.Cyber%20–%Consultancies/Privacy

ويوجد تاريخ ملئ بقضايا التقاضي الدستوري في جنوب أفريقيا، منها عدد من القضايا المتعلقة بالخصوصية.[292] على غرار المحكمة الأوروبية، وضعت المحكمة الدستورية لجنوب أفريقيا نظرية التطبيق الأفقي للحقوق بحيث يمكن تطبيق الحماية الدستورية بين الأفراد وكذلك بين الأفراد والدولة.

لا توجد حماية تنظيمية محددة للخصوصية في جنوب أفريقيا ولكن اعترفت المحاكم فيها منذ فترة طويلة بالحق في التقاضي على أساس المفهوم العام من القانون الروماني (actio iniuriarum) ومعناه الحق في التقاضي لحماية شخصية المرء. وقد فسر هذا ليشمل على النشر غير المصرح به للحقائق الشخصية (مثل الصور)، والتعدي غير المبرر على المجال الخاص والحق في الهوية الشخصية.

في وقت كتابة هذا التقرير، كانت جنوب أفريقيا ما زالت تفتقر إلى تشريعات شاملة لحماية البيانات، رغم أن هذا الأمر كان قيد الدراسة الرسمية منذ عام 2000 على الأقل. وسعى مشروع قانون حماية المعلومات الشخصية، والذي طُرح على المجلس الوطني في عام 2009،[293] إلى توفير نظام على النمط الأوروبي بشكل خاص لحماية البيانات الشخصية التي تحتفظ بها الهيئات الخاصة والعامة، مع وضع قواعد تنظم الموافقة على معالجة البيانات وتحديد أغراض استخدامها وتقييد الاستخدام لأغراض أخرى وفرض قيود على الاحتفاظ بالبيانات ووضع متطلبات لإخطار صاحب البيانات والجهة الرقابية معاً وضمان حق الوصول إلى المعلومات وتصحيحها من جانب صاحبها. كما وضعت المحكمة الدستورية إطارا أساسيا لحماية البيانات استندت فيه إلى الحماية الدستورية للخصوصية.[294] ويورد قانون الائتمان الوطني حقوق الحماية القوية للبيانات الشخصية،[295] وذلك بغية التصدي لممارسات التمييز التاريخية في القطاع المالي. وتشمل هذه الحقوق على الحق في الحصول على "معلومات سرية" على أساس الثقة، وتُستخدم فقط لغرض مشروع ولا يكشف عنها إلا للشخص الذي تتعلق به.

فيما يتعلق بالاتصالات، نجد التشريع الأساسي هو قانون تنظيم اعتراض الاتصالات والتزويد بالمعلومات المتعلقة بالاتصالات.[296] هذا القانون يشبه قوانين أخرى من حيث النوع، حيث ينص عموما على سرية الاتصالات الخاصة ثم يضع استثناءات لأسباب مختلفة، أهمها الأمن وتنفيذ القانون، وبشروط معينة. ويقتضي القانون أن يضمن مزودو خدمات الاتصالات قدرة خدماتهم على تخزين المعلومات ذات الصلة حول الاتصالات والقدرة على اعتراضها قبل أن تقدم للجمهور العام. ويشترط كذلك على مقدمي الخدمات تخزين المعلومات، وفقا لتوجيهات الوزير المسؤول، لمدة تتراوح بين ثلاث إلى خمس سنوات.

3.3 مبادرات الشركات

من الواضح أنه لابد لمبادرات الشركات أن تلعب دورا رئيسيا في أي نظام متكامل لحماية الخصوصية على الإنترنت. ففي الولايات المتحدة الأمريكية تظل هذه المبادرات بمثابة النظام الأساسي لحماية البيانات فيما يتعلق بالجهات الفاعلة في القطاع الخاص. وبموجب الأنظمة المشابهة للنظام الأوروبي، تعتبر هذه المبادرات تكميلية للقواعد الإلزامية داخليا، وغالبا ما تدعم قرارات 'الكفاية' لنقل البيانات إلى الغير. وتقتضي المادة 27 من التوجيه 95/46 أن تقوم الدول الأعضاء واللجنة الأوروبية بدعم وضع مدونات قواعد السلوك لأغراض التنظيم الذاتي، ويتم توسيع ذلك من خلال المقترحات الجديدة التي تعمل على تهيئة إمكانية وضع

---

292 أنظر بورشيل جي (Burchell, J.) "الحماية القانونية للخصوصية في جنوب إفريقيا: هجين قابل للنقل"، 13-1 المجلة الالكترونية للقانون المقارن، (مارس/ آذار2009)، ص 11-13.

293 نشر في الجريدة الرسمية بتاريخ 14 أغسطس/ آب 2009.

294 بورشيل، الحاشية 292، ص. 14.

295 رقم 34 لسنة 2005.

296 رقم 70 لسنة 2002.

آليات اعتماد لأنظمة التنظيم الذاتي، بالإضافة إلى أختام وعلامات حماية البيانات، وذلك لتمكين المستخدمين من تقييم جودة هذه الأنظمة. وقد صرح ريتشارد توماس (Richard Thomas)، مفوض المعلومات للملكة المتحدة، في ملاحظاته التمهيدية لدراسة مستقلة تناولت الاتجاهات الجديدة لحماية البيانات لأوروبا، بأنه قد يصبح من الحتمي على المدى البعيد التخلي عن القواعد وإلقاء العبء على مصدري البيانات لحماية البيانات المنقولة إلى الغير (كصورة من صور التنظيم الذاتي).[297]

في الوقت نفسه، لا تنجوا أنظمة التنظيم الذاتي من الانتقاد بذات الدرجة وذلك لعدم قدرتها على توفير الحماية الكافية لخصوصية المستخدمين في الولايات المتحدة الأمريكية حسب ما يتفق عليه الكثيرون. ووصف دان تينان (Dan Tynan) المشكلة عن طريق القياس فقال:»عندما يتعلق الأمر بصناعة الإعلانات عبر الإنترنت، يكون التنظيم الذاتي أشبه بقانون القراصنة في جميع أفلام جوني ديب: فما هي إلا مبادئ توجيهية يمكن الخروج عنها كلما دعت الحاجة إلى ذلك».[298]

وتتخذ مبادرات التنظيم الذاتي أشكالا مختلفة. وقد وضع الكثير من مزودي خدمات الإنترنت وكبرى شركات التزويد بالخدمات على الإنترنت[299] مثل جوجل وياهو والفيسبوك، سياسات الخصوصية الخاصة بكل منها. حيث وضعت شركة جوجل سياسة خصوصية جديدة دخلت حيز التنفيذ في 1 مارس/ آذار 2012.[300] وثمة خيار متصل بذلك وهو أن تجتمع الشركات في شبكة أو اتحاد واحد يتبعون فيه جميعاً سياسة خصوصية أو مجموعة معايير مركزية، ويكون شرط العضوية هو الالتزام بهذه السياسة. وهذا هو النهج الذي اعتمدته بعض المجموعات مثل جمعية التسويق المباشر (DMA)[301] وTRUSTe.[302] ويسمح للأعضاء عرض ختم أو شهادة تثبت عضويتهم والالتزام بالمعايير المشتركة.

ومن حيث الجوهر، هناك عدد من نهج السياسات، حيث تقدم معظم السياسات التزامات معينة للمستخدمين، وتسمح الكثير منها للمستخدمين الاختيار من بين بعض خيارات الخصوصية. ومن ثم تحتوي الصفحة الرئيسية من موقع الفيسبوك لدى كل مستخدم على قائمة منسدلة تقود المستخدم إلى خيارات مثل إعدادات الحساب، وإعدادات الخصوصية والخروج. وفي «إعدادات الخصوصية»، يمكن للمستخدم أن يمنع الآخرين من رؤية محتواه، أو يضع خيارات أخرى لعرض محتوى الفيسبوك، وما إلى ذلك. ومع ذلك لا يمكن للمستخدم السيطرة على استخدام الفيسبوك ذاته لبياناته الخاصة، على الرغم من تغطية سياسة الخصوصية لمختلف جوانب هذا الأمر.

في بعض الحالات، تسمح السياسات للمستخدمين اختيار عدم استخدام بياناتهم الخاصة لأغراض مختلفة، معظمها يكون للتسويق. ولذا فإن مبادرة شبكة الإعلانات (NAI)[303] توفر للمستخدمين خيار عدم الموافقة على الصفحة الأولى من موقعها، ومن ثم يمنع المستخدم من رؤية الإعلانات المصممة خصيصا للشركات الأعضاء التي اختار عدم الموافقة عليها. ولكن هذا لا يمنع وجود ملفات تعريف الارتباط على جهاز الكمبيوتر الخاص بالمستخدم أو مسح البيانات الشخصية من قواعد البيانات. وهناك خيار أكثر فعالية تستخدمه

---

297 أنظر روبينسون، جروكس، بوترمان، وفاليري (Robinson, Graux, Botterman and Valieri)، مراجعة مبادرة حماية البيانات للاتحاد الأوروبي: ملخص، الحاشية 215، مقدمة.

298 «قراصنة الخصوصية: التنظيم الذاتي هو سفينة تغرق»، 9 أغسطس/ آب 2011. متوفر على: http://www.itworld.com/it-managementstrategy/191917/privacy-pirates-self-regulation-sinking-ship.

299 وهي شركات تقدم خدمات على الإنترنت مثل الاستضافة على الإنترنت، وخدمات البريد الالكتروني والشبكات الاجتماعية ومنصات المدونات وما إلى ذلك.

300 متوفر على /http://www.google.com/policies/privacy.

301 أنظر: www.the-dma.org

302 أنظر: www.truste.org.

303 أنظر: /www.networkadvertising.org.

بعض شبكات التعرف على الوجه، مثل اتحاد الإشارات الرقمية (DSF)[304]، وشركة بوينت أوف بيرشيس أدفيرتايزنج إنترناشونال (POPAI)،[305] تقوم على خيار الانضمام، حيث من المفترض للشركات الأعضاء أن تكتسب المستخدمين باختيارهم للانضمام قبل جمع أي أنواع معينة من البيانات.

وثمة مجموعة من الأسباب الهيكلية حول الحد من فعالية التنظيم الذاتي. ومن هذه الأسباب أن العديد من الأنظمة تحمل معظم العبء على المستخدم. وبعض سياسات الخصوصية تكون طويلة ومعقدة وبلغة قانونية يصعب على المستخدم فهمها أو معرفة خيارات الخصوصية فيها. حتى وإن بذل المستخدم الجهد اللازم في فهم سياسات مزودي خدمة الإنترنت (ISP) ومزودي الخدمات على الإنترنت (OSP) التي يستخدمها بشكل دوري، فمن غير المحتمل أن يبذل هذا الجهد بالنسبة لكل الخدمات التي يستخدمها والتي قد تعرضه إلى جمع بيانات عنهأ. وفي محاولة لتسهيل الأمر على المستخدمين، أعلنت جوجل (Google) مؤخرا عن جمعها لسياسات الخصوصية على جميع الخدمات التي تقدمها بحيث يمكن للمستخدم التعرف على نسخة واحدة منها.[306] وفي معظم الحالات، يكون للهيئات الحق في تغيير سياسة الخصوصية دون إخطار المستخدم، مما يضع مزيداً من الحواجز للمستخدمين.

وثمة إشكالية أنه في حين قد توجد حوافز للعمل بطرق تراعي الخصوصية بالنسبة لبعض الشركات – وبالأخص الشركات الكبرى والمشهورة – فإن هذه الحوافز للعديد من الشركات تتأتى بطرق أخرى، وذلك لأن تحصيل هذه الشركات للأموال يكون عن طريق جمع البيانات الشخصية وبيعها. ومن المكلف تطبيق قواعد خصوصية قوية. ويكون تطبيق معظم الأنظمة ضعيفاً، ومن أسباب ذلك أن عملية المراقبة هي عملية مكلفة ونادراً ما تتم بصورة منهجية. وأخيرا، يمكن لتنفيذ سياسات الخصوصية أن تزيد في الواقع من مسؤولية الشركة، حيث تلزمها بالمسؤولية عن الإخفاق في احترام تلك السياسات.[307]

وفي الوقت نفسه، يشير العديد من المحللين إلى فوائد مختلفة ينتج عنها التنظيم الذاتي. فهو يضع المسؤولية والسيطرة في أيدي الشركات، والتي هي الأكثر احتمالاً أن تفهم مخاطر الخصوصية وتكون قادرة على تصميم حلول فعالة في بيئة معقدة جدا وسريعة التغير. ومن المرجح أن يكون التنظيم الذاتي حساساً بالنسبة لاحتياجات العمل، ويوفر المرونة التي يحتاج إليها، وذلك في سياق القطاع سريع التغير. وبعبارة أخرى، يمكن للتنظيم الذاتي أن يساعد في حماية الفوائد الاقتصادية والاجتماعية للابتكار عبر الإنترنت.

لقد تم اقتراح عدد من الأفكار لتعزيز أنظمة التنظيم الذاتي، منها توظيف الخصوصية من خلال تصميم أو بناء أنظمة الخصوصية في تصميم أنظمة الخدمات ذاتها. وهذا دون شك يبدو معقولا، ولكن لا يحل الكثير من المشاكل التي سبق ذكرها.

---

304 أنظر: /www.digitalsignagefederation.org.

305 أنظر: /http://popai.com.

306 أنظر: /http://www.google.com/policies.

307 تتعامل لجنة التجارة الاتحادية (FTC) في الولايات المتحدة، على سبيل المثال، مع انتهاكات سياسة خصوصية الشركات على أنها ممارسة متحايلة للعمل تخالف القانون. أنظر مارش (Marsh)، "تشريعات التنظيم الذاتي الفعال: نهج جديد لحماية الخصوصية الشخصية على الإنترنت" (2009) 15 مراجعة قانون الاتصالات السلكية واللاسلكية بميشيجان. 543، ص 555.

قد تكون أفكار التنظيم المشترك أكثر فعالية. فقد دعا بعض المحللين، مثل لجنة التجارة الاتحادية (FTC) في الولايات المتحدة الأمريكية، إلى فرض نظام «عدم التتبع»، على غرار قواعد "عدم الاتصال» الشعبية التي طُبقت في بعض البلدان بخصوص المكالمات الهاتفية.[308] حيث سيسمح هذا النظام للمستخدمين اختيار عدم جمع المعلومات المتعلقة بسلوكهم على الإنترنت لأغراض الدعاية المستهدفة. ويمكن تحقيق هذا، على سبيل المثال، من خلال وضع قائمة إعدادات على متصفح المستخدم لاختيار ما يفضله. وهناك احتمال آخر، وإن كان أقل صرامة في طبيعته، وهو مطالبة الشركات بالإعلان عن أي انتهاكات لسياسات الخصوصية الخاصة بها. ودعا أحد المحللين أن يمنح المشرعون مهلة سنة للشركات من أجل التوصل إلى مقترحات، ثم طلب تنفيذ النظام الأكثر فعالية من جانب كل الشركات.[309]

308 لجنة التجارة الاتحادية (FTC)، حماي خصوصية المستهلك في عصر التغير السريع: إطار مقترح لشركات الأعمال وصناع السياسة: تقرير مبدئي لفريق لجنة التجارة الاتحادية، ديسمبر/ كانون الأول 2010. متوفر على: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

309 المرجع السابق، ص 559–562.

4. استنتاجات – النقاط المشتركة بين الخصوصية وحرية التعبير

يرتبط الحق في الخصوصية بالحق في حرية التعبير ارتباطاً معقداً. وفي أمثلة عدة، يوفر احترام الحق في الخصوصية الدعم للحق في حرية التعبير كما هو الحال بالنسبة للحقوق الديمقراطية الأخرى. ولكي نعطي مثالاً واضحاً، فإن احترام سرية الاتصالات هو أمر ضروري لثقة كلٌ من يشترك في أي أنشطة تتعلق بالاتصالات، والتي تعد بدورها مطلباً رئيسياً لممارسة الحق في حرية التعبير.

ومع ذلك فإنه في حالات أخرى قد يتعارض احترام سرية البيانات مع الحق في حرية التعبير، وهذا يتجسد في مثال واضح عندما ترغب صحيفة في نشر بعض التفاصيل شديدة الخصوصية حول شخصية سياسية بارزة، وهذا بالطبع ربما يرجع إلى اعتقاد الصحيفة الراسخ في فكرها أن الإفصاح عن هذه البيانات أمر يصب في المصلحة العامة. والمثال المذكور أعلاه يعد أبرز دليل على ذلك، والذي بموجبه انتقد الكثيرون من المراقبين الحماية الفرنسية المبالغ فيها لسرية البيانات المتعلقة بفشل الإعلام وآخرون في التحقيق في ادعاءات تخص بعض التصرفات السابقة والمشكوك في صحتها التي قام بها الرئيس السابق لصندوق النقد الدولي، دومينيك ستراوس (Dominique Strauss-Kahn)– كان.

تجلت هذه العلاقات في كل من الطرق التقليدية والجديدة على شبكة الإنترنت وذلك كما هو واضح من كل من الأمثلة أعلاه (أي في أنظمة الاتصالات من خلال الإنترنت والإعلام الرقمي). هذه الموضوعات جاءت بالفعل خير عون مع التغيرات الهائلة التي حدثت في حرية التعبير والفضل يرجع في ذلك إلى شبكة الإنترنت وكافة أنظمة الاتصالات الرقمية الأخرى (مثل الهواتف المحمولة). على سبيل المثال، لقد زادت قوة الدولة على تعقب الأنشطة الفردية للأشخاص من خلال الاتصالات بدرجة كبيرة تماشياً مع الزيادة الهائلة في فرص التنقيب عن البيانات التي تتيحها النظم الرقمية.

هذا الجزء من التقرير يعمل على استكشاف طبيعة هذه العلاقات؛ حيث أنه يهتم في المقام الأول بالطريقة التي تتأثر بها حرية التعبير سلباً في ظل الضعف الذي ينتاب حماية سرية البيانات. كما أنه ينظر في التوترات بين حماية هذين الحقين، وفي بعض الحالات تحديد التهديدات التي تمس حرية التعبير التي تفرضها الحماية المبالغ فيها لسرية البيانات وفي حالات أخرى يلقي الضوء على التوترات.

1.4 أثر ضعف حماية سرية البيانات على حرية التعبير

جاءت الدوافع الأولية لحماية سرية البيانات بسبب الحالات التي شهدت تدخل الدولة في الحياة الخاصة ويظل هذا مطلباً هاماً من أجل حماية قوية لسرية البيانات على شبكة الإنترنت. لطالما كان هناك صراعاً بين الحاجة لتنفيذ القانون بشكل فعال واحترام سرية البيانات، وانعكس هذا الصرع في عدد هائل من الحالات، على الصعيد القومي في عدة دول وأمام المحاكم الدولية لحقوق الإنسان، تدعي خرق مسؤولي تنفيذ القانون لحقوق سرية البيانات. وهذا يسري بشكل واسع وواضح على الاتصالات الرقمية، ولكنها في صميم الموضوع في عدد من المجالات الأخرى التي تراعي سرية البيانات، مثل إتاحة بيانات تتعلق بالمصارف والائتمان.

لقد صار الصراع أكثر تعقيداً خلال السنوات القليلة الماضية نتيجة عدد من الاتجاهات. أولاً، كما هو ملاحظ أعلاه، من ناحية تنفيذ القانون قد زادت قيمة المعلومات المتاحة بصورة كبيرة مع تزايد قدرات التكنولوجيا الحديثة على رصد المزيد من البيانات عنا على أساس مستمر وآلي أكثر مما سبق، سواء كانت متاحة طواعية، مثلما هو الحال على صفحات الفيسبوك (Facebook)، باعتبارها جزء ضروري ولازم من تقديم الخدمة، ومثل سجل المكالمات الهاتفية من الهاتف المحمول، أو على النحو الذي تدفع به المصالح الاقتصادية وعالم المال الأعمال، مثلما تعقب أنماط الشراء التي تتم على شبكة الإنترنت. كما أن التزايد السريع لقوة التجهيز لدى الحواسب الآلية الحديثة سيكون لها أثر مضاعف.

على سبيل المثال، فإن البيانات المخزنة في الهواتف الذكية المعاصرة للمستخدم النشط تتيح وعاءً من المعلومات عن أي تحركات أو اتصالات يقوم بها المستخدم وما إلى غير ذلك. علاوة على ذلك، فإنه يتم الآن وبصورة آلية تسجيل كافة أشكال الاتصال والبحث عنها واسترجاعها بسهولة ويسر من الحاسب الآلي، مما يزيد بصورة فعالة وواسعة النطاق من فائدتها في تنفيذ القانون. وتعد الفائدة المحتملة للقدرات المتعلقة بتقنية التعرف على الوجه لاسيما مع امتزاجها بكاميرات مراقبة الفيديو في كل الأنحاء مثالاً حياً على هذا الأمر.

ثانياً، من الناحية التنظيمية والقانونية، بات من الصعب التحكم في المراقبة أكثر مما كان في الحياة التقليدية خارج الإنترنت. حيث أنه فيما مضى كانت هناك قواعد واضحة بصورة معقولة فيما يتعلق بالتصنت الهاتفي أو مراقبة ورصد الأحاديث الهاتفية رغم أنها غالباً ما تخضع لبعض الاستثناءات أو التجاهلات ولا يتم عادة تطبيقها بشكل سليم في الممارسات والتطبيقات اليومية. مثل هذا النشاط تطلب تركيب أو تفعيل معدات وأجهزة متخصصة وتوفير إجراءات محددة للرصد أو التسجيل. بمقارنة هذا مع البحث في البيانات المخزنة على هاتف محمول تمت مصادرته من مجرم مشتبه فيه. علاوة على ذلك، فإن الطرق التي يتم بها رصد وإتاحة البيانات الخاصة والسرية تتغير بصورة مستمرة، الأمر الذي يفرض بالتالي تحدياً تنظيمياً وقانونياً. ولكن هذا الأمر بدا أكثر صعوبة وتحدياً باحتمالية التعاون الطوعي فيما بين مزودي خدمة الإنترنت (ISP) ومزودي الخدمات التي تتم عبر الإنترنت (OSP) وسلطات تنفيذ القانون، والتي قد يحكمها بصورة رئيسية السياسات الخاصة بخصوصية وسرية البيانات والخاصة بمزودي الخدمة.

ثالثاً، لقد كان هناك اتجاهاً واضحاً، حتى في الأنظمة الديمقراطية، لإتاحة أنظمة قانونية تساعد على تيسير استخدام هذه المعلومات من أجل تنفيذ القانون. وعادة ما يأتي هذا من الرغبة في استخدام كافة الوسائل المتاحة لمكافحة الجريمة، بما في ذلك حقيقة أن العناصر الإجرامية غالباً ما تستغل التكنولوجيا استغلالاً فعالاً، لاسيما لأغراض الجريمة المنظمة والإرهاب. ومع ذلك، فإنه ليس من الواضح دائماً أن الاعتبارات الخاصة بسرية البيانات تؤخذ في الاعتبار بشكل كامل، ولقد تعرضت عديد من هذه الأنظمة لنقدٍ حاد من جانب المناصرين والمؤيدين لخصوصية وسرية البيانات. ويمكننا أن نأخذ التوجيهات المتعلقة بالاحتفاظ بالبيانات، والتي أبلت بلاءً سيئاً أمام المحاكم الدستورية الوطنية، مثالاً حياً على هذا. علاوة على ذلك، فإن النظم التي جاز لها أن تكتسي ملامحها بالالتزام والوفاء بالشروط حيث توافر لها وسائل حماية قوية قد تتعرض لانتهاكات خطيرة في الدول (المتعددة) حيث تكون وسائل حماية خصوصية البيانات ضعيفة.

غالباً ما يقترن ضعف وسائل حماية سرية البيانات بضعف الحماية المباشرة لحرية التعبير، الأمر الذي يؤدي إلى الأثر المضاعف. ولقد كانت هناك حالات ذات مستوى عالٍ من الأهمية حيث طلبت السلطات الصينية من مزودي الخدمات المقدمة عبر الإنترنت (OSP) إتاحة بيانات ذات طبيعة سرية من التي قد أدت إلى إدانات جنائية عن أنشطة كانت تنطوي على الحق في حرية التعبير والتي يحميها القانون الدولي.

على سبيل المثال، حكم على الصحفي الصيني شاي تاو (Shi Tao) بعشر سنوات في عام 2005 بسبب رسالة بريد إلكتروني حول إخطار حكومي بتقرير عن الذكرى السنوية لاحتجاجات تيانينمين سكوير (Tiananmen Square) التي اندلعت عام 1989. لقد أتاحت ياهو (Yahoo!) رسائل بريد إلكتروني مرسلة من حساب البريد

الإلكتروني الخاص بتاو (Tao) مرسل إلى الحكومة الصينية بناءً على طلبها. وهذه الرسائل أتاحت الأساس الذين أدين به تاو (Tao) بتهمة الإفصاح عن أسرار الدولة.[310]

في حالات عديدة، قامت دول بإتاحة أنظمة محددة بعينها من أجل التصدي للأنشطة التي تنطوي على الحق في حرية التعبير من خلال الإنترنت. ومن ثم، فإنه جاء في القانون التايلندي لارتكاب المخالفات المتعلقة بالحاسب الآلي عام 2007، والمعروف بقانون جريمة الحاسب الآلي، نصوصاً محددة حول الاحتفاظ ونشر بيانات خاطئة أو تحتوي على موادٍ إباحية، أو حتى معلومات من المرجح أن تضر بالنظام العام أو الأمن القومي، والتي قد تشمل أيضاً التعدي بالسب على الحاكم. لقد تم تطبيق هذه النصوص والأحكام على عدة حالات منذ إقرار القانون.[311] وبالمثل، يجرم قانون المعلومات والمعاملات الإلكترونية الإندونيسي رقم 2088 نشر أي أخبار خاطئة، أو أي مواد مشينة، أو إباحية عبر الإنترنت.[312] كلا النظامين قد تعرضا لانتقاد حاد للغاية من جانب نشطاء الحق في حرية التعبير.[313]

2.4 التضارب بين حرية التعبير وخصوصية البيانات

إن مسألة التضارب بين حرية التعبير وخصوصية البيانات على الإنترنت أكثر تعقيداً وتنوعاً من تلك التضاربات الناجمة عن أثر ضعف وسائل الحماية الخاصة بسرية وخصوصية البيانات على حرية التعبير. فيما أن الأخير عادة ما ينطوي على تدخلات (وغالباً معترف بها ومقرة) واضحة مع سرية البيانات، والتي عادة ما بذلت جميع الجهود اللازمة لتبريرها بسبب احتياجات تنفيذ القانون الضرورية، ومن ثم تصبح مسألة ما هو الذي يشكل سرية البيانات أمراً في غاية الحيوية والأهمية. وعلى النحو المبين أعلاه، لقد رفضت المحاكم الدولية المحلية والدولية تقديم تعريف واضح عن السرية، برغم أن الاتجاه الذي اتخذته المحاكم في الولايات المتحدة الأمريكية، والذي يتضمن عناصر شكلية (التوقع الفعلي لسرية البيانات) والموضوعية (التوقعات المعقولة لسرية البيانات)، لديه من المبررات والمسوغات اللازمة للتوصية به.

أصبح نطاق مفهوم خصوصية البيانات أمراً هاماً للغاية في بعض الحالات التي تشمل حرية التعبير. على سبيل المثال، هل يوجد لدى وزير الدفاع توقعات معقولة عن مدى خصوصية البيانات عندما يكون مدعواً على العشاء في مطعم، ولكن مع موزع أسلحة أجنبي؟ ماذا لو دُعي رئيس وزراء لحفل زفاف شخصية مشهورة؟ مما لا شك فيه أن هذا السؤال يمكن الإجابة عليه بشكل مختلف في دول مختلفة، مع وجود تداعيات هامة بالنسبة لوسائل الإعلام التي تسعى لسبق صحفي عن هذه الأنشطة.

وينبغي أن يفهم هذا الموضوع أيضاً في ضوء الإطار الرئيسي للتحديات التي تواجه حماية سرية البيانات في عالم الإنترنت والخدمات المقدمة عبر الإنترنت، وأنماط الاستجابات التنظيمية والقانونية التي أفرزتها. وفيما أوضح هذا التقرير، فإن هناك تحديات ضخمة أمام تنظيم سرية البيانات في البيئة الحالية. وتشمل هذه التحديات ما يلي:

---

310 أنظر الموقع: http://www.businessweek.com/stories/2007-11-06/jerry-yang-on-the-hot-seatbusinessweek-business-news-stock-market-and-financial-advice.

311 انظر تونساراوس، إس ومندل تي ((Tunsarawuth, S. and Mendel, T، تحليل القانون التايلاندي (2010)، متوافر على: http://www.law-democracy.org/wp-content/uploads/2010/07/10.05.Thai_.Computer-Act-Analysis.pdf.

312 قانون رقم 11/2008. انظر المواد 27، 28

313 بالنسبة لتايلاند، انظر القانون التايلاندي لجرائم الحاسب الآلي، الحاشية 2 وبالنسبة لإندونسيا، انظر الAJ، بناء حصن الحرية (2009)، بشأن ملف المؤلف.

- نموذج عمل أساسي من شأنه أن يتضمن وبصورة فعالة تبادل أو التنازل عن سرية البيانات وخصوصيتها مقابل خدمات مجانية.
- في العديد من الحالات العملية، فإن نماذج الخدمة التي تشمل الإفصاح عن المعلومات إما باعتبارها جزء مهم من النموذج (مثلما هو الحال مع الفيسبوك (Faebook)) أو لبناء الكفاءة (على سبيل المثال الأدوات التي يمكن بها ترشيد عمليات البحث القائمة على التفضيلات النموذجية للمستخدم).
- أي بيئة تنبع مما سبق والتي يمكن فيها إن أمكن وضع الحوافز، مثل الرأي العام، والتي تبذل جهداً على بعض الأعمال لاحترام سرية البيانات، فإنه يتعذر أو يصعب القيام بهذا مع عدد من الأنشطة الاقتصادية والمالية.
- أي بيئة يتعذر أو يصعب معها أن يبدي مستخدمو قواعد السرية موافقة رشيدة ومستنيرة نتيجة، من بين أشياء أخرى، مدى التعقيد الكامن في هذه القواعد، والتي يستخدمها عدد هائل من مستخدمي التطبيقات المختلفة، وانعدام واضح للاهتمام أو الوعي حول هذا بين معظم المستخدمين، أو ربما الموافقة على التبادل المنصوص عليه في النقطة الأولى أعلاه.
- الصعوبات الكامنة في حماية السرية، بما في ذلك نتيجة التدفق الهائل للمعلومات وحقيقة أنه، بمجرد «ظهور» شيئاً ما، لا يمكنك استعادتها.

لقد كان هناك فرقاً واضحاً في الاستجابة التنظيمية، لاسيما تجاه آلية حماية البيانات، في الولايات المتحدة الأمريكية (وتلك الدول التي لديها أطر مشابهة) وذلك من ناحية، وأوروبا (والدول التي تسير على نهجها) من الناحية الأخرى. لقد تبنت الولايات المتحدة الأمريكية، حيث مقر أكبر شركات مزودي الخدمات التي تقدم عبر الإنترنت، اتجاهاً واسع النطاق من الحرية في العمل، مما يحد من القوانين الخاصة بالدولة لبعض القطاعات، والتي قد أدت رغم كل ذلك إلى حماية ناقصة لخصوصية البيانات من جانب الجهات الفاعلة المنوط بها السرية والحفاظ على الخصوصية. وعلى الصعيد الآخر فقد تبنت أوروبا بصورة نسبية منهج تدخلي في عملية التنظيم ووضع القوانين، الأمر الذي جعلها عرضة للانتقادات الحادة نتيجة صرامتها المبالغ فيها، والتي تفقد الارتباط بواقع الصناعة والتي ثبت عدم جدواها وفعاليتها في حيز التطبيق (على سبيل المثال في مجال الموافقة على جمع واستخدام البيانات)، ولحد ما نتيجة هذه الانتقادات، للسماح بمساحة أكبر من التصرف والتدخل في ممارسة عدد كبير من الاستثناءات والمسئولية عن سداد جزء الأموال المستحقة.

إن حلقة الوصل الرئيسية بين هذين الاتجاهين هو برنامج اعتماد مبادئ سرية الميناء الآمن، والذي يسمح باعتماد الاتحاد الأوروبي للشركات الموجودة بالولايات المتحدة الأمريكية على أنها توفر الحماية الكافية. ولقد تعرض هذا النظام لانتقادات لعدم توفير حماية سرية البيانات على المستوى الأوروبي، الأمر الذي يبدو قضية براءات، وذلك من بين أشياء أخرى، نظراً لنقص الإجراءات الإصلاحية والعلاجية الفعالة. وعلى الجانب الآخر، فإن الحوافز الخاصة بالاتحاد الأوروبي مقابل اعتماد مزودي الخدمات عبر الإنترنت (OSP) واضحة؛ فقد يتعذر على الاتحاد الأوروبي رفض اعتماد شركات مثل الفيسبوك (Facebook) أو جوجل (Google).

وفيما يتعلق بالآثار المحددة على الحق في حرية التعبير، فإنه يمكن تحديد عدداً من المجالات المختلفة على النحو المبين أدناه.

1.2.4. المصلحة العامة

من الثابت في القانون الدولي أنه متى نشأ أي نزاع بين الحق في التعبير عن الرأي وسرية البيانات، يتعين الإشارة إلى المصلحة العامة الإجمالية كمرجعية أساسية، أو أي اختبار مماثل لهذا من أجل تقرير المصلحة الواجب تفضيلها. وهذا على سبيل المثال ثابت في اثنين من القضايا المعروضة أمام محكمة حقوق الإنسان الأوروبية وهما قضيتي فون هانوفر ضد ألمانيا (Von Hannover v. Germany).[314]

إن ممارسة توازن المصلحة العامة بين خصوصية البيانات وحرية التعبير هو أمر في صميم الموضوع في سياقين اثنين. الأول، مثلما في قضية فون هانوفر (Von Hannover)، تنشأ المشكلة عندما تكون المعلومات، رغم أنها ذات طبيعة خاصة، متاحة لوسائل الإعلام، ولكن يُنظر إلى أي نشر إضافي لهذه المواد بموجب القانون المحلي على أنه إفصاح غير منطقي عن حياة خاصة للغاية (أو ثمة أي أخطاء مماثلة). في مثل هذه الحالات، فإن الدفاع عن المصلحة العامة، سواء كان على اعتباره عنصراً من حرية التعبير عن الرأي أو كجزء من القواعد المتعلقة بالسرية، يعد أمراً بالغ الأهمية. وهكذا، في القضية الثانية الخاصة بفون هانوفر (Von Hannover)، وجدت المحكمة الأوروبية أن نشر أي بيانات شخصية خاصة بخلاف ذلك على أنه إفشاء أو اعتداء مبرر على سرية البيانات (أو نشاط محمي من خلال الحق في حرية التعبير) لاسيما بسبب أن العلاقة بين "الأسرة الحاكمة في إمارة موناكو" وأفراد من عائلته خلال المرض كانت مسألة ذات طابع عام شرعي. وللأسف الشديد فإن المصلحة العامة الأساسية في عدد من البلدان إما أن القانون لم يذكرها أو أتى على ذكرها ولكن بشكل غامض أو غير واضح.

ثانياً، ينبغي أن تؤخذ المصلحة العام في الاعتبار عند تطبيق الاستثناءات من خصوصية وسرية البيانات في الوصول للبيانات التي تحتفظ بها الهيئات العامة (الحق في الحصول على المعلومات). وهكذا، ففي إعلان مشترك تم إقراره في عام 2004،[315] أوضح المقرر الخاص التابع للأمم المتحدة المعني بتعزيز وحماية حرية الرأي والتعبير، وممثل منظمة الأمن والتعاون في أوروبا (OSCE) المعني بالإعلام، والمقرر الخاص التابع لمنظمة الدول الأمريكية المعني بتعزيز وحماية حرية التعبير في عام 2004 ما يلي:

> ينبغي أن يخضع الحق في الحصول على المعلومات إلى نظام شبه محكم ومصمم بشكل دقيق كي لا يسمح باستثناءات عريضة من أجل حماية المصالح العامة والخاصة ذات الأهمية القصوى، بما في ذلك السرية وخصوصية البيانات. وينبغي أن تسري هذه الاستثناءات فقط متى كانت هناك مخاطرة وقوع أي أضرار جوهرية على المصلحة المحمية ومتى كان هذا الضرر أكبر من المصلحة العامة العليا في القدرة على الاستفادة من المعلومات والوصول إليها.

وبالمثل، تنص إحدى التوصيات الصادرة عام 2002 عن لجنة وزراء المجلس الأوروبي[316] في المبدأ رقم 4(2) على ما يلي:

---

314 24 يونيه 2004، التماس رقم 59320/00 و7 فبراير 2012، التماس رقم 40660/08 والتماس رقم 60641/08.
أحالت المحكمة المزيد للتحقيق والتدقيق حول موضوعات وقضايا تتعلق بالمصلحة العامة، ولكن هذا يبدو على نفس النمط رغم تكييفها على الحقائق الواردة بهذه القضية

315 تم إقراره في 6 ديسمبر/ كانون الأول 2004. ومتاح على الرابط التالي:
http://www.unhchr.ch/huricane/huricane.nsf/0/9A56F80984C8BD5EC1256F6B005C47F0?opendocument

316 التوصية آر. (2002)2 – لجنة وزراء الدول الأعضاء – حول الوصول إلى والاستفادة من المستندات الرسمية، 21 فبراير 2002

> يجوز الامتناع عن إتاحة أي وثيقة أو بيانات في حالة إذا ما كان من المرجح أن يؤدي الكشف عن المعلومات أو البيانات الواردة في هذه الوثيقة الرسمية إلى الإضرار بأي من المصالح المذكورة بالفقرة رقم 1 ما لم تكون هناك مصلحة عامة ملحة وأساسية تستوجب الإعلان والإفصاح.

بالرغم أن العديد من القوانين التي تجيز حق الحصول على المعلومات تنص على المصلحة العامة العليا للاستثناءات من خصوصية وسرية البيانات، في حين أن عدد من القوانين لا تجيز ذلك.

لقد أتاحت عدة محاكم دولية بعض المؤشرات عن كيفية تحقيق التوازن بين حرية التعبير وسرية البيانات. ولقد أوضحت أن هناك افتراض قوي جداً لمصلحة حرية التعبير، وذلك بأن فكرة المصلحة العامة في هذا السياق ينبغي أن يُفهم على نطاق ضيق وأنه متى كانت هناك مصلحة عامة في نشر المعلومات، فإن الحق في التعبير عن الرأي سيعلو بالطبع على الحق في التمتع بخصوصية وسرية البيانات. والسبب في هذا واضح جلياً: إن الحق في التمتع بحرية التعبير هو مطلب رئيسي لتعزيز الديمقراطية، ولابد من حماية المناقشات التي تدور حول موضوعات تتعلق بالمنفعة أو المصلحة العامة، والتي تصب في منفعة كل فرد في المجتمع، وصيانتها حتى وإن كان من المتوقع أن تتسبب في الإضرار بخصوصية الفرد.

احتوت قضية موزلي ضد المملكة المتحدة (Mosley v. the United Kingdom) على نشر صوراً خاصة عن ماكس موزلي (Max Mosley)، والذي كان يشغل وقتئذٍ مديراً لمسابقة الفورميولا وان (Formula One)، وعن تورطه في فضائح جنسية تحت عنوان "مدير الفورميولا وان يمارس الرذيلة في حفل جنس جماعي تحمل شعار النازية مع 5 ساقطات". ولكن في نهاية الأمر فاز موزلي بقضيته أمام المحاكم البريطانية، وذلك لأحد الأسباب أهمها أن الصحيفة كانت مخطئة ولم يكن هناك أية شعارات نازية في هذا الحدث، والتي ربما قد جذبت انتباه الرأي العام وانطوى عليها جانب من المصلحة العامة. كما أنه كان قد تقدم في البداية بطلب الحصول على أمرا زجري مؤقت يقضي بمنع أي أعمال نشر أخرى عن هذا الموضوع، ولكن هذا الطلب قوبل بالرفض؛ وكان قد قدمه بالفعل مرة واحدة بعد واقعة النشر الأولى لهذه الواقعة، وبعدما مني بأضرار فادحة بالفعل. ولكن موزلي لم يتوقف عند هذا الحد، فقد واصل بعد ذلك باستئناف طلبه ولكن هذه المرة أمام المحكمة الأوروبية لحقوق الإنسان (ECHR) مدعياً بأن المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية قد انتهكت حقه في الخصوصية وذلك بأنها لم تشترط على الصحف التي تقوم بانتهاك الخصوصية بنشر الأسرار الخاصة أن تخطر الأشخاص المعنية، كي تعطيهم الفرصة للتقدم بطلب للحكم بإصدار أمراً زجرياً مانعاً ضد النشر قبل واقعة النشر الأولى (والتي عجز موزلي عن الحصول عليه).

ولكن المحكمة الأوروبية رفضت هذه الفكرة. وأفادت المحكمة في حكمها الصادر بذلك مستندة إلى المبادئ الأساسية الآتية:

> كما تؤكد المحكمة أنه لابد وأن يوجد فصل بين الإبلاغ عن الوقائع – حتى وإن كانت مثيرة للجدل – والتي من شأنها أن تساهم في إحداث جدل واسع النطاق حول أمور المصلحة العامة بشكل عام في أي مجتمع ديمقراطي، والتقدم بمزاعم أو ادعاءات قذرة أو إباحية عن الحياة الخاصة لشخص ما. وفيما يتعلق بالأولى، فإن الدور البارز للصحافة في أي نظام ديمقراطي وواجبها في العمل باعتبارها «مراقب عام» هي من الاعتبارات الهامة لصالح وضع أي قيود على حرية التعبير بصورة ضيقة ومحدودة. (تم إزالة المراجع)[317]

في قضيتي فون هانوفر (Von Hannover)، استندت المحكمة الأوروبية لحقوق الإنسان أيضاً في بعض التفاصيل على مسألة توازن حق الخصوصية والحق في حرية التعبير (وتم الاستناد إليها في المربع

---

[317] 10 مايو 2011، طلب رقم 48009/08، فقرة 114

الثالث عشر). قامت المحكمة في تلك القضايا أيضاً ونوهت بأنه متى كانت هناك مصلحة أو منفعة عامة في النشر، عادة ما يسود عندئذٍ الحق في حرية التعبير. واستندت في هذا، من بين أشياء أخرى، على موقفها الدائم أنه بالنسبة للصحافة «فإن واجبها رغم كل ذلك يتطلب – وذلك بطريقة تتماشى والتزاماتها ومسئولياتها – الإفصاح عن المعلومات والأفكار حول كافة الموضوعات المتعلقة بالمصلحة العامة».[318]

ولقد تم تطبيق نفس النهج أيضاً وبصورة واسعة النطاق عند تحقيق التوازن بين الحق في حرية التعبير والسمعة، حيث أن المحاكم الدولية وللمرة الثانية قد عولت على أهمية السماح بحرية الخطاب فيما يتعلق بأي مواد خاصة بالمصلحة العامة. وهكذا، فإنه في قضية هيريرا – أولوا ضد كوستاريكا (Herrera–Ulloa v. Costa Rica)، والتي تضمنت إدانة جنائية للتشهير، أفادت محكمة البلدان الأمريكية لحقوق الإنسان ما يلي:

في هذا السياق، من المنطقي والملائم أن أي بيانات أو إفادات صادرة بحق أي مسئول عام وشخصيات عامة أخرى تمارس أي وظائف ذات طبيعة عامة ينبغي أن تُمنح، في إطار المادة 13 (2) من المعاهدة، نطاق واسع ومحدد في الجدل العريض حول موضوعات تمس المصلحة العامة والتي تكون لازمة لإدارة أي نظام بصورة ديمقراطية حقيقية.[319]

ويمكن إيجاد الدعم اللازم لهذه الفكرة أيضاً في المادة 12(4) من قانون حقوق الإنسان الخاص بالمملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية، والتي تنص على ما يلي:

ينبغي أن تولي المحكمة اهتماماً خاصاً بالحق في حرية التعبير المنصوص عليه بالمعاهدة، ومتى تعلقت الدعاوى أو الإجراءات القانونية بالموضوعات أو المواد التي يدعيها المدعى عليه، أو التي تبدو إلى نظر المحكمة، أنها ذات طبيعة صحفية، أو أدبية، أو فنية (أو تتعلق بسلوك معين يتعلق بهذه المواد)، إلى:

(أ) درجة تكون معها:-

(1) هذه المواد قد أصبحت أو على وشك أن تصبح متاحة للعامة، أو

(2) تكون، أو ربما تكون، ذات طبيعة هامة وذات منفعة للعامة لنشرها،

(ب) أي قانون ذا صلة يتعلق بخصوصية أو سرية البيانات

2.2.4. الخصوصية مقابل حماية البيانات

هناك اختلافات على جانب كبير من الأهمية بين حماية الخصوصية في حد ذاتها وقواعد حماية البيانات، فهذا الأخير من شأنه التصدي لمشكلات معينة قد تنشأ عندما تشارك هيئات عامة أو خاصة في التجميع المنهجي للبيانات المتعلقة بالأفراد. ومن ناحية أخرى، نجد أن هناك تداخل شديد بين حماية البيانات والخصوصية، حيث رأت محاكم الدولية أن هناك عناصر معينة في أنظمة حماية البيانات قد تناولها الحق في الخصوصية.

وفي الوقت ذاته، نجد أن قواعد حماية البيانات تختلف عن الخصوصية فكلاً منهما له نطاق خاص به وتحكمه قواعد أساسية؛ فحماية البيانات تنطبق على البيانات المحددة شخصياً بينما لا تنطبق الخصوصية، على الرغم من أنه لم يتم تعريفها مطلقاً تعريفاً شمولياً، إلا على أضيق نطاق للمعلومات وعادة ما تكون هذه المعلومات هي المعلومات التي يكون الشخص لديه قدر معقول من توقع الخصوصية بشأنها. وفي نفس الوقت، نجد أن قواعد حماية البيانات أكثر محدودية بقدر ما، وبصفة عامة فإن هذه القواعد لا تنطبق إلا على المعالجة الآلية للبيانات أو معالجة مجموعات منظمة من البيانات، حيث أنه من الممكن أن تنطبق الخصوصية على أية معلومات (على سبيل المثال، تناول شخص لطعام العشاء مع شخص أخر في مطعم من المطاعم).

---

318 فون هانوفر ضد ألمانيا، 24 يونيه، 2004، الطلب رقم 59320/00، فقرة 60

319 2 يوليو، 2004، سلسلة سي. رقم 107، فقرة 128

وهذه ليست مشكلة في حد ذاتها، فعلى الرغم من التفسيرات القانونية المتباينة للحق في الخصوصية، فإن قواعد حماية البيانات لا تعترف بهيمنة المصلحة العامة. ففي حالة توجيه الاتحاد الأوربي رقم 95/46،[320] هناك حالات معينة لهيمنة المصلحة العامة تسمح بمعالجة البيانات ونقلها[321] ولكن ليس هيمنة المصلحة العامة، كما يسمح نفس النظام للدول بأن تكفل استثناء على القواعد الأساسية حيثما يتم تنفيذ معالجة البيانات لأغراض صحفية أو فنية أو أدبية وفق ما تقتضيه الحالة من أجل احترام الحق في حرية التعبير. مرة أخرى يمكن الإشارة إلي أن ذلك يكون محصور في نطاق معين ولا يغطي العديد من أشكال التعبير (كما يمكن التعليل على ذلك من خلال هذا التقرير).

ومن الناحية العملية، تعتبر هذه القضية هي القضية الأكثر إشكالية عندما يتعلق الأمر بالحق في الحصول على المعلومات، ففي العديد من البلدان هناك إما صلة قانونية على مستوى التطبيق أو ارتباك بين قواعد حماية البيانات أو الاستثناء لصالح الخصوصية في القانون الذي ينص على الحق في الحصول على المعلومات.

تتضمن أفضل ممارسة لقوانين الحق في الحصول على المعلومات تعريف لحماية الخصوصية مما يجعل من الواضح أنه لا يتم تغطية كل المعلومات المحددة، وبالتالي فإن البند 34 من قانون جنوب إفريقيا بشأن تعزيز الحق في الحصول على المعلومات[322] ينص على استثناء لمنع «الإفشاء غير المقبول للمعلومات الشخصية بشأن أي طرف ثالث»؛ كما تتضمن هذه القوانين استثناءات لاستثناء الخصوصية، على سبيل المثال عند الحصول على موافقة، فإن المعلومات في هذه الحالة تكون بالفعل معلومات عامة أو أنها معلومات تتعلق بالمهام الرسمية لموظف عام.[323]

وفي النهاية، تتضمن هذه القوانين هيمنة واضحة للمصلحة العامة بالنسبة لكافة الاستثناءات، بحيث يمكن إفشاء حتى المعلومات الخاصة حيثما يكون ذلك في المصلحة العامة من كافة النواحي. وتتسق كل هذه القواعد مع التفسير الذي تقدمه المحاكم الدولية بشأن الحق في حرية التعبير والذي بناء عليه بُني حق الإنسان في الحصول على المعلومات.

وفي نفس الوقت، في العديد من البلدان وفي ظل وجود قيود أو بدون على استثناء الخصوصية بشأن الحق في الحصول على المعلومات، تعتبر العلاقة بين الحق في الحصول على المعلومات وقوانين حماية البيانات غير واضحة وتهدف الممارسة السائدة على الأقل في بعض البلدان إلي تطبيق هذا الأخير في حالة البيانات الشخصية. وفي حالة الهند، على النقيض من ذلك، نجد أن مشروع قانون الخصوصية المقترح الذي من شأنه أن يؤسس نظام عام لحماية البيانات، لن يؤثر على النظام الذي تأسس بموجب قانون الحق في الحصول على المعلومات لسنة 2005.

3.2.4 نطاق الحماية والاختصاص القضائي

في بعض البلدان، كان هناك محاولات لتوسيع نطاق حماية الخصوصية بطريقة من شأنها أن تؤثر سلباً على حرية التعبير، كما في مثال الأرجنتين المبين أعلاه؛ حيثما تم تطبيق قواعد الخصوصية على محركات البحث على أساس أنها قادت الباحث إلي البيانات التي تنتهك الخصوصية يعد مثال جيد على ذلك. وهناك مثال أخر على حالة إيطاليا، عندما حُكم على ثلاثة مسؤولين تنفيذيين يعملون في جوجل (Google) بالسجن لمدة ستة أشهر مع إيقاف التنفيذ بسب نشر فيديو على جوجل (Google) يظهر طفل يعاني من التوحد وهو يُعامل معاملة قاسية بالرغم من حذف الفيديو فور استلام شكوى رسمية. وقد اعتبر ريتشارد توماس (Richard

---

320 انظر خطأ الملاحظة! الإشارة المرجعية غير معروفة

321 انظر المواد 7 (d) (1) 26 ،(4) 8 ،(e).

322 المادة رقم 2، 2000، متوافر على: http://www.gov.za/gazette/acts/2000/a2-00.pdf.

323 انظر بند 34 من قانون جنوب إفريقيا، نفس المرجع

Thomas)، مفوض المعلومات السابق في المملكة المتحدة لبريطانيا العظمي وأيرلندا الشمالية، هذه الحالة أمراً «سخيفاَ»[324] وقد أقامت شركة جوجل (Google) دعوى ضده على الفور.

في كلا المثالين السالف ذكرهما، من الممكن تقديم حجة معقولة بأن المؤلفين الأصليين لهذه المادة كانا مدانين بانتهاك الخصوصية. مع ذلك فإن تحميل المسؤولية لمزودي خدمة الإنترنت (OSP) عن مثل هذه المواقف، ولاسيما في حالة الممارسة على نطاق واسع، قد يجعل من الصعوبة بمكان بالنسبة لهم الاستمرار في تقديم حرية التعبير التي تعد على جانب كبير من الأهمية مما يُمكنهم من الخدمات التي يقدمونها في الوقت الراهن.

كلا المثالين ينطويان على المادة التي تتعلق بشكل وثيق بالاختصاص القضائي الذي تستند عليه المحاكم (مشاهير الأرجنتين وفتى إيطاليا)، ومع ذلك فهناك أيضاً خطر محتمل للمفاضلة بين المحاكم في قضايا الخصوصية التي شهدتها هذه المحاكم على الصعيد العالمي فيما يتعلق بالتشهير، والمعروفة تحت مسمى "سياحة التشهير"؛ وبالتالي يمكن للمدعين محاولة رفع قضايا تتعلق بالخصوصية في الاختصاصات القضائية التي يشعرون أن لديهم فيها فرصة أكبر للنجاح وحتى وإن كان اتصالهم بالاختصاص القضائي محدود والذي من شأنه تعزيز القاسم المشترك الأدنى في توازن الخصوصية وحرية التعبير.

وهناك حالة متطرفة لذلك تتمثل في قضية التشهير التي رفعها رجل أعمال سعودي ثري يُدعى خالد بن محفوظ ضد الكاتبة رايتشل إهرنفلد (Rachel Ehrenfeld)، نيويورك، حيث كتبت لمحة عنه في كتابها «تمويل الشر»: كيف يتم تمويل الإرهاب وكيف يمكن إيقافه (Funding Evil: How Terrorism is Financed and How to Stop It). وقد استمعت محاكم المملكة المتحدة لبريطانيا العظمى وشمال أيرلندا إلى القضية، بالرغم من أنه لم يُباع هناك سوى 23 نسخة من الكتاب فقط وقد حُكم غيابياً لصالح بن محفظ (في حين رفضت إهرنفلد (Ehrenfeld) الترافع في القضية).[325]

4.2.4. معلومات المحاكم

بدأت قضايا الخصوصية، أو القضايا ذات الصلة، في التأثير على الآليات التي تعتمدها المحاكم في الإفصاح عن إجراءاتها. ولا يوجد في هذا المجال سوى عدد قليل من المعايير المعترف بها، حتى على مستوى البلدان، وغالبا ما تترك القرارات في هذا الشأن لتقدير المحاكم الفردية أو نظم المحاكم. ورغم أن مبدأ العدالة المفتوحة من المبادئ الراسخة، بما في ذلك في القانون الدولي لحقوق الإنسان، عادة ما يطبق في الأساس فيما يتصل بالاطلاع على القضايا التي تنظرها المحكمة، وليس على وثائق المحكمة.

في بعض البلدان، تدخل المحاكم بالكامل ضمن الحق العام في قوانين المعلومات، ولذلك فإن انفتاحها فيما يتعلق بالوثائق أمر يحدده ذلك النظام. ومع ذلك في العديد من البلدان تكون هذه التغطية محدودة في نطاق معين وأحياناً ما تكون محصورة على المهام الإدارية للمحكمة وأحيانا ما تكون غير متضمنة للوظائف القضائية على الإطلاق.

---

324 يمكنك الرجوع إلي: http://news.bbc.co.uk/2/hi/8533695.stm.

325 يمكنك الرجوع إلي تخطيط خرائط الوسائط الرقمية: مسلسل مرجعي رقم 1: وسائط الإعلام والتشهير عبر الإنترنت (2011، مؤسسات المجتمع المفتوح). متوافر على: http://www.soros.org/sites/default/files/online-media-and-defamation-20110503.pdf

وحيث أن هناك اتجاه يكاد يكون سائداً على مستوى العالم في الهيئات العامة لزيادة المعلومات التي يقومون بنشرها على الإنترنت[326] فقد دفعت المخاوف بشأن الخصوصية بعض المحاكم، ولا سيما في الولايات المتحدة الأمريكية حيث تزيد بنسبة كبيرة هناك ممارسة المحاكم لنشر المعلومات على الإنترنت، إلي التحرك في الاتجاه المضاد. وهناك شيء واحد، على سبيل المثال يتعلق بنشر السوابق الإجرامية في الصحف المحلية وأخر يتعلق بنشرها على الإنترنت حيث أنه بعد ذلك يسهل الإطلاع عليها في أي وقت في المستقبل ومن المحتمل أن تؤثر هذه المعلومات سلباً على قدرة الشخص على الحصول على وظيفة أو إعادة الاندماج في المجتمع مرة أخرى.

ونتيجة لهذه المخاوف المتعلقة بالخصوصية، فرضت فلوريد، وهي رائدة في هذا المجال، حظراً على الجهود المبذولة لتوسيع نطاق الدخول على الإنترنت.[327] أما بالنسبة لقضية كاليفورنيا التي تتضمن رجل أعمال حصل على معلومات عن أفراد متورطين في قضايا جنائية وقام ببيعها، فإن القضية كانت تتمثل في ما إذا كان قد استطاع الدخول على سجلات الحاسوب التي تتضمن معلومات هامة بشأن المدعي عليهم، أم أنه اضطر إلي السفر إلي المحاكم الفردية للحصول على ذلك. وقد رأت المحكمة أن حقيقة كون المعلومات إلكترونية أدى إلي إثارة المزيد من المخاوف بشأن الخصوصية:

هناك فارق كبير بين الحصول على معلومات من جدول قضايا معين أو بشأن فرد معين والحصول على معلومات جدول القضايا عن أي فرد تكون الاتهامات الجنائية المدان بها معلقة في المحكمة البلدية.... إنها الطبيعة الكلية للمعلومات التي تجعلها ذات قيمة للمدعي عليه؛ وهي نفس القيمة التي تجعل نشرها من الناحية الدستورية يشكل خطراً. [328]

---

326 مرفق بالحركات الدولية الرئيسية لدعم ذلك، مثل الشراكة الحكومية المفتوحة (OGP).
يمكنك الرجوع إلي: /http://www.opengovpartnership.org

327 انظر مبادرة العدالة في المجتمع المفتوح، تقرير حو الإطلاع على المعلومات القضائية، مارس/ آذار2009.
متوافر على: http://www.right2info.org/resources/publications/Access%20to%20Judicial%20Information%20Report%20R-G%20view/203.09.DOC

328 ويستبروك في. ((Westbrook v مقاطعة لوس أنجلوس (1994)27 كاليفورنيا، التطبيق الرابع 157، ص. 16.

5. التوصيات المتعلقة بسياسة الخصوصية

يتضمن هذا التقرير دراسة متعمقة لمسألة الخصوصية على شبكة الإنترنت، من منطلق حرية التعبير، والنظر في مختلف القضايا المتعلقة بها، والمعايير الدولية والممارسات على المستوى القطري. ويتضمن هذا الجزء من التقرير توصياتنا للدول والشركات نحو ممارسات أفضل، استناداً إلى القانون الدولي والممارسات التي تتبعها الدول الأخرى، من حيث احترام الخصوصية على شبكة الإنترنت، مع الأخذ في الاعتبار التعارضات المحتملة مع الحقوق الأخرى ولا سيما حرية التعبير.

والوسائل المتبعة لتسوية التوترات بين الخصوصية وحرية التعبير بموجب القانون الدولي، كما هو موضح في الفصل السابق، هي إعطاء الأولوية للحق الذي من شأنه أن يخدم المصلحة العامة أكثر في أي قضية معينة. وبذلك، يتم تقديم مجالاً واسعاً للتقارير بشأن المسائل المتعلقة بالمصلحة العامة، التي تشمل على سبيل المثال السياسيين، حتى ولو كان هذا قد يمثل تعدياً على خصوصياتهم.

وقد أدخل ظهور الأنظمة الحديثة لحماية البيانات والتي توفر الحماية البالغة للخصوصية بعض الغموض في اختبار التوازن المنهجي بمجرد ملاحظته. ومن المهم، في هذا الصدد، التأكيد على أن حماية البيانات ليست مطابقة للخصوصية. وقد تم تصميم قواعد تنظيم حماية البيانات لمعالجة التجاوزات المحتملة المرتبطة بالمعالجة الآلية لمجموعة البيانات. وعلى الرغم من وجود تداخل كبير مع الخصوصية، إلا أنها ليست مماثلة. وتعد قواعد تنظيم حماية البيانات هي الأوسع نطاقاً حيث إنها تنطبق على جميع معلومات التعريف الشخصية، بينما تنطبق الخصوصية فقط على المعلومات التي من المتوقع أن يتواجد فيها قدر معقول من الخصوصية. وتعد قواعد تنظيم حماية البيانات هي الأقل شمولاً، حيث إنها تنطبق فقط على مجموعة البيانات، وعادة ما تخضع للمعالجة الآلية. وبالتالي، فإنها لا تنطبق على المعلومات الموجودة لدى وسائل الإعلام بموجب استقصاء أي فساد محتمل من جانب أي مسؤول.

تعتبر التفرقة أمر هام جداً حيث أنه في حين تضمن معظم أنظمة حماية البيانات عدداً من القواعد المحددة لحماية المصالح العامة المختلفة، إلا أنها لا تنص على تجاوز المصلحة العامة لقواعدها. ونتيجة لذلك، قد لا يضمن تطبيقها الاحترام التام لحرية التعبير.[329]

5.1 التدابير القانونية والتنظيمية

5.1.1. التدابير الدستورية

- ينبغي توفير الحماية الدستورية القوية لكل من الخصوصية وحرية التعبير. وينبغي أن يتضمن ذلك تدابير الحماية الإيجابية لهذه الحقوق ومن الأفضل فرض إلزام إيجابي على الدولة لتوفير الحماية ضد أي تدخل في هذه الحقوق.

329 يوجد تحليل جيد في إطار الوصول إلى المعلومات في مينديل تي (Mendel. T.) تسهيل إمكانية الوصول إلى المعلومات لأغراض البحث – دراسة استقصائية مقارنة، برنامج الأمم المتحدة الإنمائي، متوفر على: http://www.poverenik.org.rs/en/publications-/studies/1384-facilitating-access-to-information-for-research-purposes-a-comparative-survey.html.

- يجب أن ينص الدستور على قيود محدودة فقط على كل من الخصوصية وحرية التعبير. وينبغي تصميم هذا النظام بما يتكيف مع التناقضات بين هذين الحقين من خلال عملية تقييم المصلحة العامة العليا. وفي حال غياب الاعتبارات التعويضية القوية، فإن هذا سيفسر بطريقة تفتح المجال للجدل حول مسائل الاهتمام العام، حتى ولو كان هذا يتضمن الكشف عن معلومات خاصة.

يحتل الدستور قمة النظام القانوني وتتضمن معظم الدساتير لوائح أو مواثيق حقوق، بما يكفل حقوق الإنسان الأساسية. ولعله من المدهش أن الكثير من الدول التي تناولناها أعلاه لا تتضمن الحماية المباشرة للخصوصية في دساتيرها، على الرغم من قيام المحاكم بتفسير ذلك في قراراتها في الكثير من القضايا.

وعلى الرغم من هذا، فمن الواضح أن أفضل الممارسات هي توفير الحماية للخصوصية في الدستور. وعلى الرغم من ذلك، فإن من المعقد غالباً تعديل الدساتير، وهو ما يجب أن تكون عليه، ولا يتم تعديلها إلا بعد استفتاء عام على نطاق واسع، وذلك للتأكد من أن الدستور يعكس الإرادة السائدة، ويستقطب تأييداً من الشعب واسع النطاق.

لقد تبلور فهم الخصوصية منذ فترة طويلة من خلال التكنولوجيات المتاحة. بينما على الصعيد الأكثر وضوحاً تتضمن الخصوصية الحد من التعدي على الحيز المادي وحماية المسكن والممتلكات الشخصية، فإن الاهتمام المتعلق بالتحكم في المعلومات المعروفة عن الشخص هو بالضرورة جزء من التأقلم مع تأثير تكنولوجيا الاتصال.

تقوم بعض الدساتير، غالباً على أساس غير حصري، بوصف مضمون الحق في الخصوصية. فعلى سبيل المثال، يشير دستور جنوب أفريقيا بأن الخصوصية تتضمن الحق في عدم تفتيش مسكن الشخص أو أملاكه، وعدم الحجز على ممتلكاته أو اعتراض مراسلاته.[330] وبالمثل، يشير دستور نيجيريا إلى خصوصية المسكن والمراسلات وغيرها من أشكال الاتصالات.[331] ورغم أن هذه القوائم تتميز بالوضوح والشفافية، إلى إنها تمثل أيضاً تهديداً بأن البنود غير المدرجة – على سبيل المثال عدم تضمن توقع قدر معقول من الإنفراد في الأمثلة المذكورة أعلاه – قد لا يتم إدراجها. وإذا وردت إشارة محددة إلى الاتصالات، فمن الضروري توضيح أنها تغطي جميع أنواع الاتصالات، بما في ذلك مجموعة من أنواع الاتصالات التي تجرى عبر الإنترنت (رسائل البريد الإلكتروني، منشورات مواقع التواصل الاجتماعي أو المجموعات المتواجدة على الإنترنت، وعمليات الشراء، وعمليات البحث، والمواقع الالكترونية التي يتم زيارتها، الخ).

قد يكون من المفصل الإشارة ببساطة في الدستور إلى احترام الخصوصية بكل وضوح، كما هو الحال بالنسبة للوثائق الدولية الرئيسية. أو بدلاً من ذلك يمكن أن يشير الدستور إلى الخصائص العامة الرئيسية للخصوصية، مثل الخصائص الذاتية والموضوعية أو الإشارة إلى مفهوم الاستقلال الذاتي الذي يمثل أساسها. فهذه الخصائص يمكن توضيحها بشكل مباشر في الدستور أو أن تترك للمحاكم للنظر فيها.

وبموجب القانون الدولي والقانون الدستوري في العديد من الدول، تقوم حماية حقوق الإنسان على منع أي استغلال محتمل للسلطة من جانب الدولة، بدلاً من الجهات الخاصة. وفي الوقت ذاته، يعترف القانون الدولي والعديد من الدساتير بأن ذلك قد يتضمن التزامات إيجابية على الدولة لحماية الأفراد من الإضرار بحقوقهم من جانب الجهات الخاصة، وهو ما يشار إليها أحياناً باسم التطبيق الأفقي للحقوق. وبما أن هذه التهديدات تصدر عن كلا العناصر الفاعلة الرسمية والخاصة، فإن هذا يعتبر عنصراً هاماً من عناصر الحماية الشاملة للخصوصية.

---

330 المادة 14.

331 المادة 37.

الخصوصية ليست حقاً مطلقاً، كما يوضح هذا التقرير. فقد تكون محدودة، من بين أمور أخرى، بسبب احتمال تجاوزها بموجب مقتضيات تنفيذ القانون أو حقوق الغير (وذلك على سبيل المثال للبحث عن المعلومات و الأفكار وتلقيها والاعلان عليها، وهي حرية التعبير). وينبغي أن ينعكس ذلك في الضمانات الدستورية. ولضمان استمرار حماية جوهر الحق، يجب أن يضع الدستور حدوداً واضحة بشأن نطاق أية قيود على الخصوصية.

يعتبر العهد الدولي للحقوق المدنية والسياسية غير مفيد هنا، وذلك لأنه ببساطة يحمي من "التدخل التعسفي أو غير القانوني في الخصوصية"، بما لا يوفر تقريباً أي توجيهات بشأن ما هو جائز وما هو غير جائز، وتستخدم الاتفاقية الأمريكية لحقوق الإنسان لغة مشابهة. أما الاتفاقية الأوربية لحقوق الإنسان فهي أكثر تفصيلاً، حيث تفرض ثلاثة شروط على القيود، وهي أن ينص عليها القانون، وأن تكون بغرض حماية مصلحة من المصالح المذكورة، وأن تكون لازمة في مجتمع ديمقراطي لحماية تلك المصالح. وهذا يشبه كثيراً الاختبار الوارد ضمن ميثاق العهد الدولي للحقوق المدنية والسياسية والاتفاقية الأوروبية لحقوق الإنسان بشأن القيود على حرية التعبير، والتي أثبتت أهمية أن تكون قوية نسبياً كأساس لحماية تلك الحقوق.

يركز الدستور المكسيكي، في المقابل، على بعض التفاصيل المتعلقة بالحماية الإجرائية للخصوصية، حيث ينص على شروط واضحة لأوامر وعمليات التفتيش، واعتراض الاتصالات.[332] ويقتدي دستور جنوب أفريقيا أكثر بالاتفاقية الأوروبية لحقوق الإنسان، إذ يستوجب ورود بعض القيود في القانون بصورة عامة، وأن تكون «معقولة ومبررة داخل مجتمع مفتوح وديمقراطي يقوم على أساس كرامة الإنسان والمساواة والحرية»، مع الأخذ في الاعتبار العوامل المختلفة.[333]

ومن المهم أيضاً أن يكفل الدستور حماية حرية التعبير. وبموجب القانون الدولي، يتشابه نظام الاستثناءات لهذا الحق كثيراً مع النظام المنطبق بموجب الاتفاقية الأوربية لحقوق الإنسان بشأن الخصوصية؛ وخاصةً أنه يتضمن على اختبار ثلاثي الأجزاء لا يسمح إلا بالقيود التي نص عليها القانون، وما كان في حماية إحدى المصالح المذكورة وما كان ضروري لحماية تلك المصلحة.

بصرف النظر عن كيفية وضع النظام الخاص المتعلق بالاستثناءات، من المهم أن يتم وضع الحماية الدستورية لكل من الخصوصية وحرية التعبير بما بتوافق مع بعضهم البعض. وكما هو مذكور الفصل السابق، هذا يعني في الأساس أنه في حالة التعارض بين هذين الحقين، يكون العمل بمقتضى المصلحة العامة العليا.

2.1.5. الحماية في القانون المدني

ينبغي أن ينص القانون المدني على سبل الانصاف ضد الاعتداء على الخصوصية، ويتم تحديدها بشكل مناسب (إما بشكل صريح أو عن طريق تفسير المحكمة) لتغطي المعلومات المتعلقة بالفرد الذي يتوقع قدر معقول من الخصوصية.

التوافق مع المعايير الدستورية الموصى بها أعلاه، على أن تسمح هذه القاعدة بتوازن المصلحة العامة عندما يتعلق الأمر بمسألة حرية التعبير.

يجب أن توفر هذه الوسائل التعويض الملائم لكل من انتهكت خصوصيته، مع مراعاة مصالح حرية التعبير عند الاقتضاء.

---

332 المادة 16.

333 المادة 36 (1) أنظر أيضا المادة 45 من الدستور النيجيري الذي يعد مشابهاً في طبيعته.

تكون الوسيلة العملية الأساسية لحماية الخصوصية في معظم الدول من خلال دعوى مدنية يرفعها المدعون بخرق خصوصياتهم. ويكون المنطق الأساسي في ذلك أن الاعتداء على الخصوصية، مثل الاعتداء على السمعة، هو مسألة خاصة بين الأطراف المعنية، ومن ثم ينبغي أن يتم حلها عن طريق القانون المدني. ومن ثم تكون هذه هي الطريقة الأقرب من الناحية العملية لضمان حماية هذا الحق.

في الكثير من الدول، يضع القانون السبب القانوني لإقامة الدعوى ضد انتهاك الخصوصية. وفي دول أخرى، يكون سبب التداعي هذا جزء من سبل قانونية أوسع نطاقاً. وهكذا، في دول القانون العام، والتي تتبع النظام القانوني للمملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية، تم استخدام دعوى خرق الثقة للتعويض عن انتهاك الخصوصية، بينما في كثير من دول القانون المدني، والتي تعتمد نظمها القانونية على المدونات القانونية التفصيلية، قد تم استخدام مفهوم القانون الروماني دعوى المصلحة الخاصة (actio iniuiarum) في هذا الشأن.

إن اشتراط الدعوى المدنية ضد انتهاكات الخصوصية يعتبر على نحو بيّن من أفضل الممارسات، ويشكل التزاماً قانونياً بموجب القانون الدولي (وفي كثير من الدساتير).[334] وبغرض التوضيح، قد يكون من الأفضل النص على حماية صريحة لهذا الحق، على الرغم من اعتراف المحاكم الدولية بأن دعوى خرق الثقة قد توفر الحماية الكافية للخصوصية.[335]

لا تحدد العديد من قوانين حماية الخصوصية تعريفاً واضحاً للخصوصية، ولقد أشرنا إلى إشكالية عدم وجود تعريف محدد. وفي الوقت ذاته، من الضروري الإشارة إلي أن الخصوصية تختلف عن التعريف الشخصي لها (والذي يعتبر هو المعيار المستخدم في قواعد حماية البيانات). عوضاً عن ذلك، يوجد مفهوم توقع قدر معقول من الخصوصية في عدد من الولايات القضائية – بما في ذلك فرنسا[336] وكندا[337] وأستراليا[338] – وتم الإشارة إلى هذه الفكرة من خلال الاتفاقية الأوربية لحقوق الإنسان.[339] ويبدو أنه تم وضع قيود عامة صارمة بشأن نطاق هذا المفهوم (في حالة عدم توافر هذا التوقع المعقول لدى الشخص، فمن المؤكد أنه لا يمكن الدفاع عن الأمر بأنه من الخصوصية). وتوجد الكثير من القيود المحددة بشأن نطاق الخصوصية في قوانين مختلفة – على سبيل المثال إذا وافق الشخص على الإفصاح، فالمعلومات تعتبر عامة بالفعل أو إذا كانت المعلومات تتعلق بالوظائف العامة لمسؤول ما – وتعتبر هذه القيود بمثابة استفاضة محددة للفكرة العامة بتوقع قدر معقول من الخصوصية.

334 انظر، على سبيل المثال، التعليق العام 16 للجنة المعنية رقم 16 للجنة حقوق الإنسان التابعة للأمم المتحدة، والحق في احترام الخصوصية، والأسرة والمسكن والمراسلات وحماية العرض والسمعة (المادة 17)، 8 إبريل 1988.

335 انظر ايرل سبنسر وكونتيس سبنسر ضد المملكة المتحدة (Earl Spencer and Countess Spencer v. the United Kingdom)، 16 يناير/ كانون الثاني 1998، العريضة رقم: 28851/95 و العريضة رقم: 28852/95 (اللجنة الأوروبية لحقوق الإنسان). منذ ذلك الوقت، صاغت المحاكم في المملكة المتحدة سببا مباشرا لدعوى انتهاك الخصوصية من قانون خرق الثقة. انظر كامبل ضد إم جي إن إل تي دي ليمتد [2004] 2 إيه سي 457، الفقرة 51.

336 أنظر شنايدر ضد ستي يونيون إيديشنز مودرنز (Schneider v. Sté Union Editions Modernes)، 5 يونيو 1979، باريس محكمة الاستئناف.

337 أوبري ضد إيديشنز فايس فيرسا إنك (Aubry v. Éditions Vice-Versa Inc.) [1998] 1 SCR 591، الفقرة. 57 وما يليها.

338 أوستراليان برودكاستينج كوربوريشن ضد لينه جيم ميتس بي تي واي لميتد (Australian Broadcasting Corporation v. Lenah Game Meats Pty Ltd) [2001] إتش سي إيه 63 (15 نوفمبر/ تشرين الثاني 2001)، الفقرة. 42.

339 فون هانوفر ضد ألمانيا (Von Hannover v. Germany)، 24 يونيو 2004، العريضة رقم: 59320/00، الفقرة 51.

في الولايات المتحدة الأمريكية، نتج عن انتهاك الخصوصية توفير الحماية التجارية في الأساس من انتحال اسم الشخص أو الشبه. ولكن في الدول الأخرى تم التمييز بين الخصوصية باعتبارها قضية استقلال شخصي والمصالح التجارية الناشئة عن التحكم في المعلومات الخاصة. وظهرت هذه القضية في المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية في قضية دوغلاس ضد هيلو! ليمتد (Hello! Ltd)، والتي تضمنت النشر غير المصرح به لصور من حفل زفاف مايكل دوغلاس (Michael Douglas) بكاثرين زيتا جونز (Catherine Zeta–Jones) من قبل مجلة هيلو! (Hello!)، عندما قامت ببيع هذه الحقوق الحصرية لمجلة أخرى، وتسمى أوكى! (OK!) اعتبرت محكمة الاستئناف في المملكة المتحدة أنه على الرغم من أنهم قد وافقوا على نشر صور لزفافهما، إلا أن المدعين الفرديين يحتفظون بالحق (الجزئي) في الخصوصية وذلك لأنهم في أغلَبِ الأحيان لديهم حق الاعتراض على نشر الصور من قبل أوكى! (OK!)، وهو ما لا يمكن ضد مجلة هيلو! (Hello!)[340] وكذلك قضت المحكمة بشكل منفصل بأن لهما مصلحة تجارية محفوظة. وهناك اختلافات شديدة بين هذين النوعين من المصالح – أي الخصوصية والقيمة التجارية – وذلك ضمن أمور أخرى لأن الخصوصية مكفولة بموجب القانون الدولي لحقوق الإنسان. وتظهر هذه الاختلافات لتسمح بالتعامل المتباين مع هذه المصالح في القانون.

من المسائل المهمة نطاق الانصاف من انتهاك الخصوصية، خاصة عندما يتضمن الأمر حرية التعبير، وهو الأمر غير المتكرر. وتعتبر التعويضات المالية هي الأكثر شيوعا للانصاف. فبموجب القانون الفرنسي، يوجد التعويضات الأخرى، بما في ذلك الحجز على المواد المسيئة وقد تكون هناك سبل أخرى مناسبة لإيقاف التعدي على الخصوصية. في قضية دوغلاس ضد هيلو! ليمتد (Douglas v. Hello! Ltd)، رفضت محكمة الاستئناف في المملكة المتحدة منح إنذار قضائي ضد نشر الصور، وذلك، من بين أمور أخرى، لأن أوكي! (OK) قد تحصل على تعويض تجاري من هيلو! (Hello!) من خلال الإدعاء القضائي، ويحتفظ المدعي الفردي بحقه في مصلحة محددة للخصوصية، (بعد بيع معظم حقوق الخصوصية).[341] وفي الأرجنتين، قد تمنح المحاكم تعويضات وتأمر بوقف النشاط المتعدى به على الخصوصية، وعند الاقتضاء، تأمر بنشر الحكم.

بموجب القانون الدولي، حتى إذا كان من المناسب تقييد الحقوق، فإن فرض عقوبات مشددة، في حد ذاته، يشكل انتهاكاً للحقوق.[342] نتيجة لذلك، وحتى عندما تتغلب مصلحة الخصوصية على الحق في حرية التعبير، يجب أن يؤخذ نطاق الانصاف في الاعتبار (أي يجب أن يكون الانصاف أيضاً متناسباً).

---

340 دوغلاس و أورس ضد هيلو ليمتد وأورس (Douglas & Ors v Hello Ltd. & Ors) [2005] EWCA Civ 595 (18 مايو 2005)، الفقرة 109. وفي قضية سابقة لدى محكمة الاستئناف حول إمكانية إصدار إنذار قضائي ضد النشر من قبل هيلو! (Hello!) صرح القاضي سيدلي (Sedley): "وإذا كان كل ما حدث أن مجلة هيلو! (Hello!) تسيطر على صور مجلية أوكي! (OK)، فإن للأخيرة الحق في التعويض بموجب القانون، ولكن أعتقد بأن السيد/ دوغلاس (Douglas) والسيدة/ زيتا جونز (Zeta–Jones) لن يطالبا بالتعويض عن انتهاك الخصوصية التي شاركا فيها بالفعل". دوغلاس وأنور ضد نورثورن آند شل بي إل سي وأنور (Douglas & Anor v Northern And Shell Plc & Anor) [2000] EWCA Civ 353 (21 ديسمبر/ كانون الأول 2000)، الفقرة 140.

341 دوغلاس وأنور ضد نوثورن وشل بي إل سي وأنور ((Douglas & Anor v Northern And Shell Plc & Anor [2000] EWCA Civ 353 (21 ديسمبر/ كانون الأول 2000)، الفقرة 144.

342 انظر، على سبيل المثال، تولستوي ميلوسلافيسكي ضد المملكة المتحدة (Tolstoy Miloslavsky v. United Kingdom)، 13 يوليو 1995، العريضة رقم: 91/18139 (المحكمة الأوربية لحقوق الإنسان).

3.1.5. الحماية في القانون الجنائي

- يجب على الدول أن تضع قواعد جنائية لكل قطاع بشأن الخصوصية، وذلك لحماية بعض المعلومات الحساسة للغاية، مثل خصوصية الاتصالات والمعاملات المصرفية.
- في حين أن هذه الحماية لا ينبغي أن تكون مطلقة، وذلك على سبيل المثال عندما تكون مراقبة الاتصالات السلكية واللاسلكية أمراً ضرورياً لأغراض تنفيذ القانون، ينبغي أن يكون هناك قيود قوية إجرائية (أي تتطلب عادة أمر قضائي) وموضوعية (مثل إثبات ضرورة التدابير في التحقيق في جريمة خطيرة).
- تجنب فرض أي حظر جنائي عام على التعدي على الخصوصية من المرجح أن يتعارض مع الحق في حرية التعبير.

وهناك بعض الدول – مثل الصين والأرجنتين والولايات المتحدة الأمريكية – التي تطبق حماية جنائية محدودة للخصوصية، وبالأخص عن طريق حظر نشر أنواع معينة من المعلومات القطاعية (على سبيل المثال فيما يتعلق بالاتصالات السلكية واللاسلكية أو المعاملات المصرفية). بالإضافة إلى هذه الدول المرشحة، وضعت بعض الدول مخططات إجرامية لمعالجة مشاكل معينة.[343] وفي بعض الحالات، تقتصر هذه القواعد الجنائية على المعلومات التي يحتفظ بها المسؤولون، بينما في حالات أخرى تنطبق على القطاع الخاص.

وفي عدد قليل من البلدان – ولا سيما في فرنسا – هناك قيود جنائية أكثر عمومية بشأن التعدي على الخصوصية. فبالنسبة لفرنسا، قد وضعت العديد من هذه القواعد الجنائية خصيصاً للتصدي لسلوك مصوري المشاهير وحتى استخدام وسائل الإعلام لمحتوى صور المشاهير. ومن ثم نصت المادة 226–1 من قانون العقوبات على تجريم تعمد انتهاك الحياة الخاصة لشخص آخر دون موافقته عن طريق، من بين أمور أخرى، "التقاط صورة لشخص في مكان خاص أو تسجيلها أو إرسالها".

للنهج القطاعي دور يُحمد عليه، وذلك بقدر ما يتعين توفير حماية قوية لفئات معينة من المواد الخاصة بسبب مخاطر الجرائم (الأخرى) أو الأخطاء المدنية التي ترتكب في حال عدم حمايتها. وربما المثال الأكثر وضوحاً على ذلك هو المعلومات المصرفية. ولكن تدل تجربة العديد من البلدان على أنه ليست هناك حاجة لوضع فعل جرمي عام يتمثل في انتهاك الخصوصية، وتعد هذه إشكالية خاصة عند تطبيق هذه القواعد للحد من حرية التعبير.

وبموجب القانون الدولي والقانون المعمول به في العديد من البلدان، لا يمكن إزالة هذه الحماية إلا عند وجود مصلحة عامة ملحة تبرر ذلك. ومن الأمثلة التقليدية على ذلك تنفيذ القانون (وذلك عندما يصرح للشرطة مراقبة الاتصالات السلكية واللاسلكية كجزء من التحقيق في جريمة من الجرائم). وينبغي أن يكون هناك حواجز إجرائية وموضوعية لإزالة هذه الحماية. فمن حيث الإجراءات، لابد أن يتم ذلك بأمر قضائي؛ ومن حيث الموضوعية، لابد من وجود دليل واضح على المصلحة العامة العليا التي تقتضي ذلك، مثل التحقيق في جريمة من الجرائم الخطرة.

343 من الأمثلة الجيدة على ذلك قانون حماية خصوصية السائق بالولايات المتحدة الأمريكية لسنة 1994، 18 مدونة الولايات المتحدة، الفصل 123، تم اعتماده استجابة إلى اتساع بيع المعلومات الشخصية الموجودة في سجلات المركبات.

4.1.5. أنظمة حماية البيانات

- ينبغي على الدول وضع أنظمة قوية لحماية البيانات تشتمل على السمات الرئيسية المذكورة أدناه، وهي إمكانية التطبيق على نطاق واسع، والحق في الموافقة، والحق في الوصول والتصحيح، والالتزامات على المتحكمين في البيانات، والحق في التعويض.
- يجب أن يكون هناك استثناءات لهذه القواعد بخصوص أنواع معينة من جمع البيانات، ولا سيما عندما يكون ذلك لأغراض حرية التعبير.
- وبخلاف ذلك، يتعين حل أي تنازع بين حرية التعبير، بما في ذلك الحق في المعلومات، وقواعد حماية البيانات وفقاً للنظام الدستوري من أجل حل التضارب بين حرية التعبير والخصوصية، أي من خلال القرارات التي تفضل المصلحة العامة العليا. وينبغي أيضاً أن تكون سبل الانصاف متناسبة.

لقد أصبح من المتفق عليه بشكل واسع أن أنظمة حماية البيانات هي عنصر أساسي من الحماية الأوسع للخصوصية، وبعض عناصر هذه الأنظمة هي مكفولة بموجب القانون الدولي لحقوق الإنسان. وعليه بدأت الدول الديمقراطية بصورة متزايدة بوضع هذه الأنظمة موضع التنفيذ. ويرد وصف الخصائص الرئيسية لهذه الأنظمة في المربع 15.[344] تشتمل الملامح الرئيسية لأي نظام حماية قوي على ما يلي:

(1) **إمكانية التطبيق على نطاق واسع–** ينبغي أن تطبق هذه القواعد على مجموعات البيانات الشخصية والمتحكمين في البيانات في كل من القطاعين العام والخاص.

(2) **الحق في الاختيار / الموافقة –** يجب أن يمنح للفرد حرية الموافقة على جمع معلوماته من عدمه، مع وجود بعض الاستثناءات المحدودة عند وجود مصلحة عليا يقررها القانون لجمع هذه المعلومات. وهذا يعني فهم الأفراد وإعلامهم بإخطار واضح يتضمن ممارسات جمع المعلومات التي تنتهجها الجهة العامة أو الخاصة قبل مباشرتها لجمع أي معلومات شخصية؛ على أن يوضح هذا الإخطار نوع المعلومات المقترح جمعها والاحتفاظ بها، والقائم بجمعها، وطريقة استخدامها، ومن له الحق في الوصول إليها. ولابد كذلك أن يكون صاحب البيانات على دراية بما إذا كان التزويد بالمعلومات المطلوبة أمر اختياري أم بحكم القانون؛ ولا يجوز استخدام المعلومات لأي أغراض تتنافى مع الأغراض التي جمعت من أجلها.

(3) **الحق في الوصول إلى المعلومات والتصحيح –** ينبغي أن يكون للفرد الحق في الوصول إلى المعلومات التي يُحتفظ بها عنه على فترات معقولة ودون تأخير لا مبرر له. وينبغي كذلك أن يكون له الحق في أن يطلب من المتحكم في البيانات تصحيح أي أخطاء أو مسح أي بيانات، عند الاقتضاء.

(4) **مسؤوليات المتحفظ بالمعلومات –** يجب أن يتخذ المتحكمون في البيانات خطوات معقولة لضمان دقة وسلامة المعلومات لديهم. وينبغي أن توضع قيود على الوصول إلى البيانات وفقاً للاستخدامات المقررة للبيانات. ويجب عدم نقل البيانات إلى الأطراف الثالثة إلا بعد ضمان التزامهم أيضاً بمبادئ حماية البيانات. وينبغي إتلاف البيانات بمجرد الاستغناء عنها للاستخدامات المحددة، أو تحويلها إلى شكل مجهول. ويراعى اتخاذ الخطوات الملائمة أثناء الاحتفاظ بالبيانات لضمان سريتها وسلامتها وجودتها.

(5) **الحق في التعويض –** يجب أن يُمنح الأفراد الحق في التعويض ضد كل من الهيئات العامة والخاصة التي لا تحترم قواعد حماية البيانات فيما يتعلق بالبيانات الخاصة بهم. ويمكن توفير سبل الانصاف من خلال التنظيم الذاتي ودعاوي القانون الخاص والإجراءات الحكومة. وينبغي أن تقوم هيئة مستقلة بالرقابة على النظام.

---

344 على الرغم من أن هذا المربع يصف نظام حماية البيانات في الاتحاد الأوروبي من الناحية الرسمية، إلا إنه يمثل ممارسة أفضل في هذا السياق.

تشتمل الأنظمة الأفضل لحماية البيانات على استثناءات لمعالجة البيانات المتعلقة بممارسة حرية التعبير (وإن وصفت في بعض الأحيان وصفاً ضيقاً على نحو غير ملائم لأغراض صحفية وفنية مع استبعاد وسائل التعبير الأخرى، مثل نشر الكتب). ولهذا أهمية تتمثل، من بين أمور أخرى، في التعريف واسع النطاق للبيانات الشخصية المستخدمة في هذه الأنظمة (بيانات تحديد الهوية) وعدم وجود مبادئ تحكم الاستخدام (أي أن لأنظمة تنفيذ المصلحة العامة أن تتجاوز ذلك).

حتى عندما تنطبق قواعد حماية البيانات، ينبغي حل التعارض بين الخصوصية وحرية التعبير وفقاً للقواعد الدستورية العامة لمعالجة مثل هذا التضارب. وبعبارة أخرى، ينبغي إجراء تقييم للمصلحة العامة العليا.

هناك مسألة يحتمل أن تكون أكثر تعقيداً، وهي العلاقة بين أنظمة حماية البيانات والوصول إلى المعلومات. وهنا أيضاً ممارسة أفضل تتمثل في الاعتماد على الحماية العامة للخصوصية ووضع تعريف لها، بدلاً من القواعد المتخصصة في نظام حماية البيانات، والتي لم تصمم لتوفير توازن مناسب عام بين الوصول والسرية في مجال الخصوصية. وبما أن الحق في الحصول على المعلومات هو جزء من الحق في حرية التعبير بموجب القانون الدولي، فإن هذا النهج يتسق مع النقطة السابقة (من ناحية تحقيق التوازن بين حرية التعبير والخصوصية)، ويتسق كذلك مع المبادئ الأساسية للحق في المعلومات، بما في ذلك وجوب إتاحة المعلومات بشكل عام عندما يكون ذلك في المصلحة العامة العليا، حتى وإن نتج عن ذلك إضرار بالمصلحة المحمية، مثل الخصوصية.

5.2. سياسة وممارسات الشركات

- يجب على الشركات وضع سياسات خصوصية قوية لحماية المستخدمين، وينبغي أن تكفل هذه السياسات، كمبدأ عام، أكبر قدر ممكن من السيطرة على الخصوصية للمستخدمين وأن تتضمن قواعد لتغيير السياسة بما يكفل الحماية للمستخدمين ضد زيادة تعرضهم لعمليات التعدي على الخصوصية. وسنعرض هذا النهج المحتمل لهذه السياسات بالمزيد من التفاصيل أدناه.
- لابد من الاهتمام الأكبر بتطوير المبادرات ذات التنظيم الذاتي وربما ذات التنظيم المشترك، فضلاً عن الخيارات التعاونية، لحماية خصوصية المستخدمين. وينبغي على الشركات تخصيص مزيداً من الوقت والموارد لهذه القضية الهامة بالتشاور مع المعنيين الآخرين.
- يجب على الشركات التعهد بالتزام عام لحمل قضايا الخصوصية وحرية التعبير على محمل الجد. وسوف يعتمد ما يعنيه هذا من الناحية العملية على الأنشطة الخاصة بكل شركة، ولكن ينبغي على الأقل أن تخصص الشركة بعض الوقت والطاقة للتفكير في أساليب يمكن أن تتكيف مع عملياتها من أجل تعزيز احترام هذه الحقوق الأساسية. وفي معظم الحالات، ينبغي أن يتضمن هذا عملية وضع سياسة شفافة.

كما نلاحظ في أماكن أخرى من هذا التقرير أن المبادرات ذات التنظيم الذاتي للشركات تمثل تحدياً بالنسبة للخصوصية لأن جميع حوافز الأعمال لمزودي خدمات الإنترنت (ISP) ومزودي الخدمات من خلال الإنترنت (OSP) هي ضد الخصوصية، بصرف النظر عن الرأي العام الذي ينطبق بقوة على عدد قليل من الشركات. ونتيجة لذلك، انتقد الكثير من المراقبين جهود التنظيم الذاتي.[345]

وفي الوقت ذاته، تعتبر ممارسات الشركات الجيدة أمراً ضرورياً للنجاح في حماية الخصوصية على الإنترنت. ولعل أهم جانب من هذه الجوانب يتعلق بالموافقة، التي بمجرد منحها يتم التنازل بشكل فعال عن أهم قواعد حماية البيانات. وغالباً ما يقوم المستخدمون من خلال آليات القبول بالموافقة على سياسات الخصوصية

---

345 بعض هذه الأمور مذكرة أعلاه. أنظر الحاشية 298 والنص المتعلق بها.

ونهجها (غالباً ما تكون أقل رسمية) بشأن خصوصية مزودي خدمات الإنترنت ومزودي الخدمات على الإنترنت. وكما أشرنا، ثمة تحديات متعددة أمام تطبيق هذه الأنظمة، بما في ذلك التعقيد (ربما الضرورة) للسياسات/النهج، والعدد الكبير من الخدمات المختلفة التي يستخدمها الأفراد وتدني مستوى مشاركة المستخدمين بشأن هذه المشكلة. وتظهر كذلك مسألة تغيير الشركات لسياسات خصوصياتهم. كل هذا ينقل وبشكل فعال قدر كبير من السيطرة، وبالتالي من المسؤولية، إلى الشركات.

ويمكن تحديد عدد من أفضل الممارسات لسياسات الخصوصية. أولاً، يجب أن تلتزم الشركات بوضع سياسات خصوصية واضحة تستند بشكل عام على معايير احترام الخصوصية المفصلة في هذا التقرير. الكثير من مزودي خدمات الإنترنت ومزودي الخدمات من خلال الإنترنت ليس لديهم هذه السياسات. يجب أن تكون هذه السياسات سهلة الاستخدام، مثلاً يجب أن يكون من السهل الوصول إليها على الإنترنت وأن تكون مكتوبة بأكبر قدر من الوضوح والسهولة.

ثانياً، يجب أن يمتلك المستخدم السيطرة على الخصوصية كلما أمكن – وكذلك عندما يتسق هذا مع الخدمة المقدمة ونموذج الأعمال الأساسي للشركة. على سبيل المثال، يجب أن تسمح شركة الفيسبوك (Facebook) للمستخدمين وضع بعض خيارات الخصوصية على الأقل فيما يتعلق بما يستطيع المستخدم الآخر رؤيته، وأن توفر جوجل (Google) العديد من خيارات الانسحاب والانضمام.[346] وبقدر ما تتطلب خيارات الانضمام من الاهتمام البالغ من جانب المستخدم، فهي إجراء مفضل من منظور الخصوصية.

ثالثا، ينبغي على الشركات تقديم التزامات معينة للمستخدمين بشأن التغييرات على سياسات الخصوصية الخاصة بها. حيث تعد جوجل (Google) بعدم التقليل من خصوصية المستخدمين دون موافقتهم الصريحة. وتعد شركة الفيسبوك (Facebook) بالسماح للمستخدمين بتقديم تعليقاتهم لمدة 7 أيام على معظم التغييرات، وإذا تقدم أكثر من 7.000 شخص بتعليقات، مع العلم بأن إجمالي عدد المستخدمين ليس بالضرورة عائقاً مستحيلاً، يُطرح الأمر للتصويت، ويكون التصويت ملزماً بطريقة أو بأخرى في حال مشاركة 30% من جميع المستخدمين المسجلين.[347] وهذا يشكل عائقاً كبيراً جداً (أي انخفاض معدلات المشاركة حتى في الانتخابات الوطنية في معظم البلدان) ولكن ربما ليس بالدرجة المستحيلة عندما يكون التغيير مثيراً جداً للجدل.

لا يزال النقاش حول سياسات الشركات في هذا المجال في بدايته من بعض الجوانب. ولابد من بذل المزيد للخروج بأفكار واختبارها والموافقة على نهج أفضل الممارسات. ولمعالجة بعض أوجه القصور التي تنطوي عليها البرامج ذات التنظيم الذاتي أو القائمة على حوافز الشركات، طالب بعض المحللين إطلاق مبادرات ذات تنظيم مشترك تشارك فيها الشركات ومنظمات المجتمع المدني والحكومات. ولابد من فعل المزيد للتأكد مما إذا كانت هذه الأفكار مجدية ومما إذا كانت ما تشكله من مخاطر يفوق ما تجنيه من فوائد للمصالح التي تسعى إلى دعمها، أي احترام الخصوصية وحرية التعبير.

يمكن لفكرة الترتيبات التعاونية أيضاً أن تكون مجدية، حيث إن التعاون يختلف عن التنظيم المشترك في طبيعته التطوعية، ويتشابه معه من حيث تغطية كلا من القطاعين العام والخاص. والفكرة الواعدة هنا هي الاعتماد الرسمي لمزودي الخدمات. وقد يتضمن هذا الاتفاق مجموعة من المعايير الأساسية ومن ثم اعتماد الشركات التي تفي بهذه المعايير. ويمكن استكشاف خيارات متعددة بشأن الرقابة على النظام، وذلك إما من خلال هيئة عامة مستقلة، مثل أجهزة الاتصالات السلكية واللاسلكية في كثير من البلدان، أو هيئة قطاعية، وقد يستوجب الأمر وضع ترتيبات تعاونية مختلفة لتنفيذ القواعد.

وعلى الرغم من وجوب فعل المزيد من العمل بشأن هذه المسائل، إلا أنه في الوقت نفسه تسعى بعض الشركات إلى تطوير خيارات أفضل لسياسة حماية الخصوصية على الإنترنت. ومن الأمثلة على ذلك شركة موزيلا

---

346 السياسة متوفرة على: /http://www.google.com/policies/privacy

347 السياسة متوفر عل: /http://www.facebook.com/about/privacy.

(Mozilla)، التي تزود بمتصفح فايرفوكس (Firefox).[348] فبناء على نهج شركة موزيلا، يوجد مجموعة من المبادئ المحتملة التي تقوم عليها سياسة الشركات بشأن الخصوصية على النحو التالي:

(1) **عدم المفاجآت**. يجب على الشركات والخدمات استخدام وجمع وتبادل المعلومات حول المستخدمين وفقاً فقط لما هو مبين في إشعارات واضحة وموجزة وسهلة الفهم.

(1) **الخيارات الحقيقية**. يجب على الشركات والخدمات منح المستخدمين خيارات عملية ومفصلة من خلال توفير معلومات واضحة عند جمع المعلومات وإتاحة خيار الانسحاب كلما كان ذلك ممكناً.

(1) **إعدادات معقولة**. يجب على الشركات والخدمات إنشاء إعدادات افتراضية في المنتجات والخدمات توازن بين الخصوصية والأمن وخبرة المستخدم.

(1) **بيانات محدودة**. يجب على الشركات والخدمات جمع المعلومات والاحتفاظ بها بما لا يتجاوز ما هو ضروري لتنفيذ الغرض أو المهمة ولتلبية توقعات المستخدم المعقولة بشأن الخصوصية. ويراعى استخدام البيانات المجمعة غير المحددة الهوية كلما كان ذلك ممكناً، ويتم الاحتفاظ بالمعلومات الشخصية خلال مدة احتياجها للغرض الذي جُمعت من أجله فقط.

(1) **تحكم المستخدم**. يجب على الشركات والخدمات عدم تتبع أو الكشف عن المعلومات الشخصية للمستخدم دون موافقته. ويجب توظيف تعزيزات للخصوصية تمكن الأفراد من التحكم في معلوماتهم ومن فهم كيفية استخدامها ووقف جمعها وتتبع معلوماتهم الشخصية أينما أرادوا ذلك.

(1) **وصول المستخدم**. يجب أن يكون للمستخدمين الحق في معرفة متى يتم جمع البيانات الخاصة بهم أو معالجتها وحق الوصول إلى هذه البيانات بشكل مفهوم. وينبغي تقديم هذه المعلومات إلى المستخدمين مجاناً ويجب أن تكون لديهم القدرة على حذف أو تصحيح الأخطاء الموجودة في المعلومات.

(1) **الأطراف الثالثة الموثوق بها**. يجب على الشركات والخدمات أن تجعل من الخصوصية عاملاً رئيسياً في اختيار الشركاء والتفاعل معهم. وبالإضافة إلى ذلك، يجب على جميع الشركات والخدمات الأخرى أن تلتزم بهذه المبادئ لصون الخصوصية.

(1) **الأمن**. يجب على الشركات والخدمات اتخاذ التدابير المناسبة لحماية البيانات ضد المخاطر الطبيعية والبشرية على حد سواء، بما في ذلك الوصول غير المصرح به أو إساءة الاستخدام أو الخطأ. وفي حال اختراق موقع الكتروني أو خدمة أمن على شبكة الإنترنت، يكون للمستخدمين الحق في معرفة ذلك على الفور.

(1) **شفافية مشاركة الحكومة**. يجب على الشركات والخدمات إعلام المستخدمين بطلبات الحكومة للحصول على معلومات ترتبط بحساباتهم عندما يجيز لهم القانون القيام بذلك، مع منح المستخدمين حق الاعتراض على هذا الطلب متى اختاروا ذلك.

(1) **توفير سبل الانصاف:** إذا علمت الشركة أو الخدمة بأنها تسببت أو شاركت في إحداث تأثيرات سلبية على خصوصية المستخدم، يتعين عليها ضمان أو المشاركة في ضمان التعامل مع الشكاوى وتوفير سبل الانصاف للمستخدمين المتضررين من خلال عملية تتسم بالشفافية.

(1) **الخصوصية في جميع المجالات**. يجب ضمان حماية الخصوصية لجميع أنظمة الإنترنت والهاتف المحمول وجميع الشركات والخدمات والتطبيقات الخارجية. ويجب أيضاً على الشركات ضمان التزام شركائها بمبادئ خصوصية قوية.

---

348 .http://www.mozilla.org/about/policies/privacy-policy.html

إن التضارب المحتمل مع حرية التعبير يثير الكثير من القضايا الصعبة لمزودي خدمات الإنترنت ومزودي الخدمات من خلال الإنترنت. فالشركات التي تعمل في العديد من البلدان التي لا يضمن فيها الإطار القانوني حماية قوية لحرية التعبير غالباً ما تواجه خيارات صعبة، مثل ياهو! (Yahoo!) في الصين، كما ذكر أعلاه. وحتى تتجنب مواجهة هذه الخيارات، انسحبت جوجل (Google) بشكل فعال من بر الصين الرئيسي في مارس/ آذار 2010.[349]

وفي العديد من البلدان الأخرى، ثمة عدد من الخيارات أمام الشركات، بدءاً من النهج «الأكثر صرامة» مثل استخدام الإطار القانوني في الإصرار على الحقوق ضد الحكومات التي تسعى للانتقاص من الخصوصية و/ أو حرية التعبير، إلى استخدام نفوذها (وخاصة بالنسبة لكبرى الشركات الدولية) في توظيف نهج أقل صرامة ولكن فعالة جداً على الدوام مثل تطبيق أنظمة تعزز من الوعي بالحقوق بين الموظفين وأعضاء هياكل الإدارة، وتبادل المعلومات حول المشاكل والحلول، ودراسة المخاطر وتصميم الحلول والردود واستعراض التقدم المحرز. والكثير من هذه الإجراءات مفصل في المبادئ التوجيهية لتنفيذ مبادرة الشبكة العالمية (GNI).[350] ويعتمد الكثير من هذه الإجراءات على الإرادة السياسية، التي تبدو للأسف متدنية إلى حد ما بين مزودي خدمات الإنترنت (IPS) ومزودي الخدمات من خلال الإنترنت (OPS)، كما هو واضح في أن مبادرة الشبكة العالمية (GNI) لا يزال بها خمسة أعضاء من الشركات.

5.3. رفع مستوى الوعي

- يجب أن تلتزم الدول ببذل جهود لرفع مستوى الوعي بشأن الخصوصية والتقنيات الجديدة، والتي تستهدف الشباب من خلال النظام المدرسي وباستخدام نظم أخرى للوصول إلى الكبار.
- يجب على الجهات الفاعلة الأخرى التي يمكنها وضعها من رفع مستوى الوعي – مثل الشركات وأولياء الأمور ومؤسسات المجتمع المدني – أن يؤدوا دوراً في تعزيز فهم أفضل بين الجمهور العام حول الخصوصية والتقنيات الجديدة.
- ثمة دور حيوي لوسائل الإعلام في رفع مستوى الوعي حول أهمية الخصوصية وظهور التحديات المختلفة مع تطور شبكة الإنترنت. وتظهر الأحداث الأخيرة في المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية عندما تم اختراق الهاتف المحمول لضحايا الجريمة وأدى ذلك إلى إغلاق صحيفة هي الأكثر مبيعاً في المملكة المتحدة، تظهر مدى الضرر الذي يلحق بالسمعة نتيجة نقص الوعي بكيفية احترام الخصوصية على شبكة الإنترنت. ولابد للصحفيين أن يدركوا ويعملوا على رفع مستوى الوعي بالآثار المترتبة على وسائط التقنيات الجديدة ومدى انتهاكها للخصوصية. في الوقت نفسه، يجب أن تكون وسائل الإعلام على دراية بمدى افتقار الضوابط باسم الخصوصية للضمانات الكافية لحماية حرية التعبير.

لا يمكن لأي مجموعة من التوصيات حول الخصوصية وحرية التعبير على شبكة الإنترنت أن تكتمل دون الإشارة إلى الجمهور العام، أي المستخدمين الرئيسيين للإنترنت. حيث يمكن فعل المزيد من قبل المستخدمين لحماية خصوصياتهم وحريتهم في التعبير على الإنترنت. حتى مع سهولة استخدام الأجهزة المتطورة جداً، مثل أدوات التشفير، فإن رفع مستوى الوعي بجوانب بسيطة تتعلق بطبيعة التقنيات الجديدة يمكن أن تساعد المستخدمين على تجنب الوقوع في فخاخ الخصوصية. على سبيل المثال، معرفة أن بعض أصحاب العمل يستخدمون الإنترنت للبحث عن خلفية الموظفين المحتملين قد يؤدي إلى مزيد من الحذر في وضع ضوابط الخصوصية على الفيسبوك (Facebook).

---

349 أنظر إعلان جوجل (Google) على: http://googleblog.blogspot.ca/2010/03/new-approach-to-china-update.html.

350 متوفر على: http://globalnetworkinitiative.org/implementationguidelines/index.php.

يجب أن يكون الإلمام بكيفية استخدام الوسائط والإنترنت من المهارات الحياتية الأساسية في النظام التعليمي، بدءاً من سن مبكرة جداً وكجزء من التعليم المدني الأوسع أو دورات التنمية البشرية. وينبغي للدول أيضاً توجيه جهود التوعية حول الخصوصية والتكنولوجيا الجديدة إلى البالغين، على سبيل المثال من خلال تطوير مصادر رفع مستوى الوعي وتوفيرها على الإنترنت وفي أماكن أخرى يمكن للبالغين الوصول إليها.

ويمكن أيضاً للعديد من الجهات الفاعلة الاجتماعية الأخرى أن تلعب دوراً في هذا الشأن. فيجب على مزودي خدمات الإنترنت (ISP) ومزودي الخدمات من خلال الإنترنت (OSP) بذل جهود لتسليط الضوء على المخاطر المحتملة بشأن «اللامبالاة» بالخصوصية على المستخدمين، مع الاعتراف بأنه قد يصعب على الشركات تحذير العملاء المحتملين من مخاطر استخدام الخدمات الخاصة بهم. وينبغي على وسائط الإعلام معالجة هذا الأمر كجزء من واجبها العام لإعلام الناس بالمسائل ذات الاهتمام العام. وتعمل العديد من منظمات المجتمع المدني على قضايا تمثل الخصوصية على الإنترنت بالنسبة لها أمراً حيوياً، وينبغي أن تتضمن مبادرات رفع مستوى الوعي في عملها. وينبغي كذلك تشجيع الآباء على القيام بدور في هذا الصدد من خلال حماية الأطفال بتوعيتهم من مخاطر الخصوصية على شبكة الإنترنت. إن هذه مهمة كبيرة، ولكن بتضافر جهود كل المعنيين، يمكن تحقيق أفضل النتائج.

مصادر مفيدة

تتضمن هذه الوثيقة معلومات تم جمعها حول الخصوصية على الإنترنت وحرية التعبير، وتم تنظيم هذه المعلومات حتى تغطي المناطق الخمس التالية: أفريقيا، وآسيا والمحيط الهادئ، وأمريكا اللاتينية ومنطقة البحر الكاريبي، والدول العربية، وأوروبا وأمريكا الشمالية. وبالإضافة إلى ذلك احتوت الوثيقة على قسم يركز بوجه خاص على نوع الجنس في النهاية. وتم العثور على الوثائق والتقارير والكتب والأبحاث من المكتبات الأكاديمية وكذلك من خلال كبرى المنظمات غير الحكومية والمراكز الأكاديمية التي تهتم بهذه القضايا. وفي الأقسام العامة والإقليمية، تم ترتيب أولوية الوثائق ووضعت على رأس القائمة الخاصة بها. وتم الانتهاء من البحث في 6 يوليو/ تموز، وحتى ذلك الحين كانت جميع الروابط نشطة.

6.1 مصادر عامة

بانيسار دي، ودافيس دي (1999) (Banisar, D. and Davies, D.)، "التوجهات العالمية في حماية الخصوصية: دراسة استقصائية دولية عن قوانين وتطورات الخصوصية وحماية البيانات والمراقبة"، متوفر على: http://www.jcil.org/journal/articles/117.html

فارس آر، وانغ إس، وبالفري جي (2008) (Faris, R., Wang, S. and Palfrey, J.)، ابتكارات "الرقابة 2.0": التكنولوجيا\الإدارة\ العولمة، متوفر على: http://www.mitpressjournals.org/doi/abs/10.1162/itgg.2008.3.2.165

لانواس بي. (2011) (Lanois, P.) "الخصوصية في عصر السحاب"، صحيفة قانون الإنترنت، رقم التسلسل الدولي: 1094–2904، 12/2011، مجلد 15، إصدار 6، ص. 3.

بامبور دي، بالفري جيه، زيتراين جيه (2004) (Bambauer, D., Palfrey, J., and Zittrain, J) "نقطة البداية: الآثار القانونية المترتبة على تنقية الإنترنت"مبادرة الشبكة المفتوحة، متوفر على: http://opennet.net/docs/Legal_Implications.pdf

بويد دي (2010) (Boyd, D.). (عيش الحياة وسط العامة) لماذا اختار الشباب الأمريكي العمومية على الخصوصية. "رابطة باحثي الإنترنت. جوتنبرج، السويد، متوفر على: http://www.danah.org/papers/talks/2010/AOIR2010.html

بويد دي (2010) (Boyd, D.)." تقبل العقل للخصوصية والعمومية". SXSW" أوستن، تكساس" متوفر على: http://www.danah.org/papers/talks/2010/SXSW2010.html

بويد دي (2010) (Boyd, D.). "الخصوصية والعمومية في سياق الكثير من البيانات". رالي، إن سي، NC متوفر على: http://www.google.com.ar/url?sa=t&rct=j&q=20%20publicity%20and%22privacy%in20data&source=web&cd=1&ved=0CGAQFjAA&url=http%20big%20of%20context%20the%2FWWW2010.html&ei=cTD3T_fS%2F2010%2Ftalks%2Fpapers%2Fwww.danah.org%2F%3A%E4OE8ASPw8TuBg&usg=AFQjCNHvgZNDYr_f3a28tOWhUIHFyHdq4A

بويد دي (2010) (Boyd, D.). "الخصوصية و العمومية والوضوح". "تيك فيست بحث مايكروسوفت، في ريدموند، واشنطن.

بويد دي (2010) (Boyd, D.). "مستقبل الخصوصية: كيف يمكن أن تثرى معايير الخصوصية اللائحة." المؤتمر الدولي لحماية البيانات ومفوضي الخصوصية. القدس، اسرائيل، متوفر على: http://www.danah.org/papers/talks/2010/PrivacyGenerations.html

بويد دي (2010) (Boyd, D.)." الخصوصية في الشبكات" منتدى الديمقراطية الشخصية. نيويورك، 6 يونيو/ حزيران، متوفر على: http://www.danah.org/papers/talks/2011/PDF2011.html

بويد دي ومارويك، إيه (2011) (Boyd, D. and Marwick, A). " الخصوصية الاجتماعية بين جمهور الشبكات: اتجاهات الشباب وممارساتهم واستراتيجياتهم." ورقة تم إعدادها من جانب معهد الإنترنت في أكسفورد، ندوة بعنوان عشر سنوات في زمن الإنترنت، المنعقدة بتاريخ 22 سبتمبر/ أيلول، متوفر على: http://www.danah.org/papers/2011/SocialPrivacyPLSC-Draft.pdf

بويد دي ومارويك إيه (2011) (Boyd, D. and Marwick, A). " علم إخفاء المعلومات الاجتماعية: الخصوصية بين الجمهور المرتبط بالشبكات" الرابطة الدولية للاتصالات. بوسطن، متوفر على: http://www.danah.org/papers/2011/Steganography-ICAVersion.pdf

برونتون، إف ونيسنبوم، إتش (2011) (Brunton, F., and Nissenbaum, H.)، "المقاومة العامة لجمع البيانات والتحليل: نظرية سياسية للتعتيم"، الأثنين الأول (فرست مانداي)، مجلد 16، رقم 5، متوفر على: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3493/2955

ديبرت، أر. (2000) (Deibert, R.)، مذهب فعالية المواطن، الإنترنت والسياسة العامة الدولية"، آفاق الدراسات الدولية، مجلد1، رقم 3، صفحة 255-272.

ديبرت،أر. (2003) ،(Deibert, R.)، "القانون الأسود:الرقابة، المراقبة، إدخال النظام العسكري في فضاء الإنترنت،" الألفية: صحيفة الدراسات الدولية، مجلد 32، رقم 3.

ديبرت،أر. (2004) ،(Deibert, R.)،"الجدران النارية والطاقة: لمحة عامة حول الرقابة الدولية العالمية على الإنترنت،"من خلال نارت فيلنوف في كلانج وإم وموراي، إيه (Nart Villeneuve in Klang, M. & Murray, A)، (محرران)، حقوق الإنسان في العصر الرقمي، كافنديش للنشر لندن.

إي إف إف (2011) ،(EFF)، "حرية التعبير والخصوصية والغفلية على الإنترنت. التعليقات المقدمة إلي المقرر الخاص للأمم المتحدة بشان تعزيز وحماية الحق في الرأي والتعبير" متوفر على: https://www.eff.org/sites/default/files/filenode/UNSpecialRapporteurFOE2011-final_3_0.pdf

فارس، أر وزيتراين، جيه. (2009) ،(Faris, R. and Zittrain, J.) "تكتيكات الشبكة العنكبوتية" الفهرس الخاص بالرقابة، 38:90، متوفر على: http://ioc.sagepub.com/content/38/4/90.full.pdf+html

فراندا، إم. (2002) ،(Franda, M)، الإنترنت والفضاء الالكتروني، تطوير الإنترنت والسياسات القائمة في مناطق العالم الخمس، شركة ناشري لين رينر(Lynne Rienner)، الولايات المتحدة الأمريكية والمملكة المتحدة، متوفر على: http://books.google.com.ar/books?hl=es&lr=&id=k89jJKN1wXcC&oi=fnd&pg=PR11&dq=privacy+and+Internet+arab+region&ots=aYTBncvUIw&sig=4vOeAgHxO5UWD20region&f=false%20arab%20internet%20and%quGdba1EE18Kks#v=onepage&q=privacy

مبادرة الشبكات العالمية، (2010)، التقرير الافتتاحي، 2010. عملنا. رؤيتنا. تطورنا، متوفر على: http://www.globalnetworkinitiative.org/files/GNI_Annual_Report_2010.pdf

هارتذوج، دبليو. (2009) (Hartzog, W)، "صندوق الخصوصية: مقترح البرنامج" الأثنين الأول (فرست مانداي)، مجلد 14، العدد 11- 2، متوفر على: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2682/2361

منتدى حوكمة الإنترنت، (2012)، تطوير المستقبل معاً، تم التعديل بواسطة بريان غوترمان، الاجتماع الخامس لحكومة الإنترنت، فيلنيوس، ليتوانيا، متوفر على: http://www.intgovforum.org/cms/2011/book/IGF_2010_Book.pdf

ليون، بي، أور، بي.، بالباكاو، أر، كرانور، إل.، شاي، أر ووا، واي (Leon, P., Ur, B., (Balebako, R., Cranor, L., Shay, R. and Wa, Y، (2011). "لماذا لم يستطع جوني الاختيار: تقييم مدى إمكانية استخدام الأدوات للحد من الإعلان السلوكي على الإنترنت"، متوفر على: http://www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html

إعلان مدريد الخاص بالخصوصية، (2011)، متوفر على: http://thepublicvoice.org/madrid-declaration/

مارويك، إيه.، مرجيا دياز، دي وبالفري، جيه. (2010)، (.Marwick, A., Murgia Diaz, D., and Palfrey, J)، "الشباب والخصوصية والسمعة"، متوفر على: http://cyber.law.harvard.edu/publications/2010/Youth_Privacy_Reputation_Lit_Review

بالفري، جيه. (2008) (.Palfrey, J)، "العام والخاص على حدود الولايات المتحدة مع الفضاء الإلكتروني"، متوفر على: http://cyber.law.harvard.edu/publications/2008/Public_and_Private_at_US_Border_with_Cyberspace

بالفري، جيه وروجويسكاي، أر. (2006)، (Palfrey, J. and Rogoyski, R)، "التحرك نحو الوسط: التهديد الدائم بالكلام الضار لحيادية الشبكة"، جامعة واشنطن، صحيفة القانون والسياسة.

الخصوصية الدولية (2012)، تقييم اتفاقية مراقبة السفر المبرم بين الاتحاد الأوربي والولايات المتحدة، متوفر على: https://www.privacyinternational.org/reports/an-assessment-of-the-eu-us-travel-surveillance-agreement

راينس – جولدي، كيه. (Raynes-Goldie, K)، "الأسماء المستعارة وتغيير الشكل وتنظيف الجدران: فهم الخصوصية في زمن الفيس بوك" الأثنين الأول (فرست ماندای)، المجلد 15، عدد 1-4، متوفر على: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432

رودريغيز، كيه. (2012)، (Rodriguez, K)، "جوازات السفر وبطاقات الهوية الوطنية الإلكترونية: شعور زائف بالأمان"، متوفر على: https://www.eff.org/deeplinks/2012/06/biometrics-national-id-passports-false-sense-security

الجمعية العامة للأمم المتحدة، (2012)، تعزيز حقوق الإنسان وحمايتها والتمتع بها فيما يتعلق بالإنترنت»، متوفر على: http://www.regeringen.se/content/1/c6/19/64/51/6999c512.pdf

فان دن بيرغ، بي وفان دير هوف، إس. (2012)، (Van den Berg, B. and Van der Hof, S)، ماذا حدث لبياناتي؟ نهج جديد لإخبار المستخدمين بممارسات معالجة البيانات"، الأثنين الأول (فرست ماندای)،

مجلد 17، عدد 7، متوفر على: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/4010/3274.

فان شويك، بي. (2012) ،(Van Schewick, B)، "حيادية الشبكات وجودة الخدمات :ماذا يجب أن تشبه قاعدة عدم التمييز"، متوفر على: http://cyberlaw.stanford.edu/publications

فيلنوف، إن. ((Villeneuve, N، (2006)، "مصفوفة التنقية: الآليات المدمجة لمراقبة المعلومات وتخطيط الحدود في الفضاء الإلكتروني" الاثنين الأول (فرست مانداي)، مجلد 11، متوفر على: http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1307/1227

فولوخ، إي. (1999) ،(Volokh, E)، "حرية التعبير وخصوصية المعلومات وردود الأفعال المزعجة حول الحق في إيقاف الناس عن الحديث عنك"، متوفر على: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=200469

زيتراين، جيه. (2003) ،(Zittrain, J)، "نقاط مراقبة الإنترنت" استعراض القانون كلية بوسطن، متوفر على: http://cyber.law.harvard.edu/publications/2003/Internet_Points_of_Control

زيتراين، جيه. (2003) ،(Zittrain, J)، كن حذراً عندما تسأل عن: التوفيق بين عالمية الإنترنت والقانون المحلي"، (PDF)، من يحكم الإنترنت؟ معهد كاتو، متوفر على: http://cyber.law.harvard.edu/node/367

زيتراين، جيه. (2006) ،(Zittrain, J)، "الإنترنت المولد"، استعراض قانون هارفارد، مجلد 119، ص.1974، مايو 2006، متوفر على: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=847124

6.2. إفريقيا

ثابانج ماست، إن. (2012) ،(Thabang Masete, N)، "التحديات القائمة في حماية الخصوصية المالية في جنوب إفريقيا"، صحيفة القانون التجاري الدولي والتكنولوجيا، رقم دولي معياري تسلسلي: 1901–8401، 07/2012، مجلد 7، إصدار 3، باور بوينت –248 259

أولينجر، إتش، بريتز و أوليفير، إم (2007)، (Olinger, H., Britz, J. and Olivier, M)، " الخصوصية الغربية أو أوبونتو؟ بعض التعليقات الانتقادية على التأثيرات في مشروع قانون خصوصية البيانات الوشيكة في جنوب إفريقيا"، مراجعة المعلومات الدولية والمكتبة، رقم دولي معياري تسلسلي: 1057–2317، 2007، مجلد 39، إصدار 1، باور بوينت –31 43

ميفول، كيه وتيرنر، سي. (2011) ،(Mivule, K. and Turner, C)، "تطبيق تقنيات خصوصية البيانات على البيانات المجدولة في أوغندا"، متوفر على: http://arxiv.org/abs/1107.3784

مبادرة الشبكة المفتوحة (2009)، «تنقية الإنترنت في إفريقيا جنوب الصحراء الكبرى»، متوفر على: http://opennet.net/sites/opennet.net/files/ONI_SSAfrica_2009.pdf

نكوبي، سي، (2004) ،(Ncube, C)، "التحليل التنافسي لأنظمة حماية البيانات في كلاً من زيمبابوي وجنوب إفريقيا"، صحيفة المعلومات والقانون والتكنولوجيا، متوفر على: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_2/ncube/caroline.doc

بانيسار، دي. (Banisar, D)، (2009)، "سياسات تكنولوجيا المعلومات والاتصالات المتعلقة بالخصوصية وحرية التعبير والحصول على المعلومات: دراسة ملخصة" جامعة ماكيريري، حقوق الإنسان ومركز السلام"، متوافرعلى: http://idl-bnc.idrc.ca/dspace/handle/10625/34234

بونيفاس ماكيليلو، إيه. (Boniface Makulilo, A)، (2012)، حماية الخصوصية والبيانات في إفريقيا: حالة الفن، صحافة جامعة أكسفورد، متوفر على: http://idpl.oxfordjournals.org/content/early/2012/06/11/idpl.ips014.full

كوهين، تي. (Cohen, T)، (2000)، "أما بالنسبة لدقة قرع وطلب حق الدخول: قانون المراقبة وحقوق الخصوصية في جنوب إفريقيا"، متوافرعلى: http://idl-bnc.idrc.ca/dspace/handle/10625/42079

فارس، أر. وربروتس، إتش وهيكوك، أر وزوكرمان، إي وجاسر، إي (Faris, R., Roberts, H., Heacock, R., Zuckerman, E. and Gasser, E)، (200×)، "أمن الإنترنت في الشرق الأوسط وشمال إفريقيا. استقصاء حول التصورات والمعرفة والممارسة" قانون هارفارد للإنترنت، متوفر على: http://cyber.law.harvard.edu/node/6973

IDRC، "حماية خصوصية الشباب في أمريكا اللاتينية"، متوفر على: http://www.idrc.ca/EN/Programs/Science_and_Innovation/Information_and_Networks/Pages/ResultDetails.Aspx?ResultID=60

كوفي – أرما، دي (Kofi-Armah, D)، أمن الإنترنت وكمية البيانات في غانا، إفريقيا: منظور هاكر، متوفر على: http://www.connectedafrica.com/internet-security-and-data-protection-in-ghana-africa-a-hackers-perspective-interview-with-sepo/

ماكينون، أر وريسن، تي وحسين إتش ولي، دبليو ولوزي، جيه مايرز، إس (MacKinon, R., Risen, T., Hussain, H., Li, W., Losey, J. and Myers, S)، (2012)، تقرير مستخدمي الإنترنت: طبعة التدخل، الأصوات العالمية على الإنترنت، تم الإرسال بتاريخ 14 يونيو/ حزيران 2012، متوفر على: http://advocacy.globalvoicesonline.org/2012/06/14/netizenreport-intervention/

ماكيليلو، إيه (Makulilo, A)، (2012)، "حماية الخصوصية والبيانات في إفريقيا: حالة الفن"، القانون الدولي لخصوصية البيانات، متوفر على: http://idpl.oxfordjournals.org/content/early/2012/06/11/idpl.ips014.abstract

الخصوصية الدولية (2006)، جنوب إفريقيا، متوفر على: https://www.privacyinternational.org/reports/south-africa

6.3. الدول العربية

الديواني، إيه. إم (Aladwani, A.M)، (2003)، الخصائص الرئيسية للإنترنت وقضايا التجارة الإلكترونية، تكنولوجيا المعلومات والناس، مجلد 16، إصدار 1، ص. 9 – 20، متوفر على: http://www.emeraldinsight.com/journals.htm?articleid=883574&show=abstract

أرف، بي وفنسنت، بي (Warf, B. and Vincent, P)، (2007)، الجغرافيات المتعددة للإنترنت في الدول العربية، مجلد 39، إصدار 1، ص. 83 – 96، مارس/ آذار 2007، متوفر على: http://onlinelibrary.wiley.com/doi/10.1111/j.1475-4762.2007.00717.x/full

الرشيد، إيه. (2001)، «الإنترنت في المملكة العربية السعودية»، متوفر على: http://www.isu.net.sa/library/CETEM2001-AlRasheed.pdf

مكتب الديمقراطية (2007)، حقوق الإنسان والعمل، العراق، الولايات المتحدة، وزارة الخارجية الأمريكية

بوركهات، إي (1998) ،(Burkhart, E)، "الأمن القومي والإنترنت في منطقة خليج فارس"، متوفر على: http://www.georgetown.edu/research/arabtech/pgi98-10.html

مسيحه، إن (2011) ،(Messieh, N)، "اكتشف العربية الرقمية: استخدام الإنترنت في الشرق الأوسط بالأرقام"، متوفر على: http://thenextweb.com/me/2011/08/25/discover-digital-arabia-middle-east-Internet-usage-in-numbers/

نعمان، إتش (2009) ،(Noman, H)، "لمحة عامة حول الديموغرافيات وأنماط استخدام مستخدمي الإنترنت في البلدان النامية: عدد مستخدمي الإنترنت في اليمن باعتبارها دراسة حالة"، برنامج الأمم المتحدة الأنمائي، متوفر على: http://opennet.net/sites/opennet.net/files/ONI_Yemen_2009.pdf

مبادرة الشبكة المفتوحة (2004)، «تنقية الإنترنت في المملكة العربية السعودية، متوفر على: http://opennet.net/studies/saudi

مبادرة الشبكة المفتوحة (2005)، «تنقية الإنترنت في البحرين خلال 2004– 2005» متوفر على: http://opennet.net/studies/bahrain

مبادرة الشبكة المفتوحة (2005)، «تنقية الإنترنت في إيران خلال 2004 – 2005: دراسة قطرية»، متوفر على: http://opennet.net/studies/iran

مبادرة الشبكة المفتوحة (2005)، «تنقية الإنترنت في الإمارات العربية المتحدة خلال 2004 – 2005: دراسة قطرية، متوفر على: http://opennet.net/studies/uae

مبادرة الشبكة المفتوحة (2005)، «تنقية الإنترنت في اليمن خلال 2004 – 2005 : دراسة قطرية، متوفر على: http://opennet.net/studies/yemen

مبادرة الشبكة المفتوحة (2004)، «تنقية الإنترنت في المملكة العربية السعودية، متوفر على: http://www.opennetinitiative.net/studies/saudi/#toc4c

الخصوصية الدولية (2006)، الإمارات العربية المتحدة، متوفر على: https://www.privacyinternational.org/reports/united-arab-emirates

الخصوصية الدولية (2006)، العراق، متوفر على: https://www.privacyinternational.org/reports/united-arab-emirates

أرهوزينسكاي، أر (2004) ،(Rohozinski, R) "الوكلاء السريين والإخوان المتخفين: ثورة المعلومات الخفية في العالم العربي"، متوفر على: http://mediaresearchhub.ssrc.org/201csecret-agents201d-and-201cundercover-brothers201d-the-hidden-information-revolution-in-the-arab-world/attachment

سيت، إس وعلى، إس والطويل، كيه وسناء الله، إس (2010) (Sait, S., Ali, S., Al-Tawil, K. and Sanaullah)، "اتجاهات استخدام الإنترنت وتأثيراته الاجتماعية في المملكة العربية السعودية"، متوفر على: http://www.google.com.ar/url?sa=t&rct=j&q=saudi%20internet&source=web%20privacy%20arabia%

2Fric%2Fsadiq%2Fcoe%2Ffaculty.kfupm.edu.sa%2F%3A%&cd=5&ved=0CGcQFjAE&url=http
2FSocialEffectsTrends.doc&ei=-CL3T_-yM4aQ8wSi0KSJBw&usg=AFQjC%2Fdoc%2Frich%hfiles
NGL6f6FgAK5e1hDNLiEaXff8QcwpA

زيتران والدمان (Zittrain & Edelman)، "وثائق تنقية الإنترنت في المملكة العربية السعودية"، متوفر على:
http://cyber.law.harvard.edu/filtering/saudiarabia/sa-yahoo-3.html

6.4. آسيا ودول الباسيفيك

مبادرة الشبكة المفتوحة (2009)، «تنقية الإنترنت في آسيا»، متوفر على: http://opennet.net/sites/opennet.net/files/ONI_Asia_2009.pdf

تشونغ، أر (2003)، (Chung, R)، بطاقة الهوية الذكية الخاصة بهونج كونج: قضايا خصوصية البيانات وانعكاساتها ما بعد أحداث 11 سبتمبر/ أيلول في أمريكا، صحيفة قانون دول الباسيفيك وآسيا والسياسة؛ مجلد 4، إصدار 2

جهو، دبليو (2005)، (Jho, W) "تحديات الحكومة الالكترونية: احتجاجات المجتمع المدني على حماية الخصوصية في الحكومة الإلكترونية في كوريا"، متوفر على: http://ras.sagepub.com/content/71/1/151.abstract

جوميز، جيه. (2003) (Gomez, J.)، "إلغاء الديمقراطية: اتجاهات نحو وضع تنظيم عمل الإنترنت، والمراقبة، والرقابة في آسيا"، استعراض سريع لصحافة دول الباسيفيك متوفر على:

http://gomezcentre.academia.edu/JamesGomez/Papers/116683/Dumbing_down_democracy_trends_in_internet_regulation_surveillance_and_control_in_Asia

كيتياديساي، كيه. (2005)، (Kitiyadisai, K.)، "حقوق وحماية الخصوصية: القيم الأجنبية في السياق التايلاندي المعاصر"، الأخلاقيات وتكنولوجيا المعلومات"، متوفر على: http://www.stc.arts.chula.ac.th/feeds/Krisana/7156321v361p0324.pdf

تشيك، دبليو. (Chik, W.)، "الأسد والتنين والدولاب نحو حراسة الطريق نحو سرية المعلومات والاتصالات على الإنترنت: دراسة عملية مقارنة لهونج كونج وسنغافورة - "اتجاهين آسيويين مختلفين"، الجريدة الدولية للقانون وتكنولوجيا المعلومات، الرقم الدولي المعياري التسلسلي، 0769-0967، 04/2006، العدد 14، الإصدار رقم 1، الصفحة رقم 47

جرينليف، جي. (2012)، (Greenleaf, G.)، "وعود وأوهام حماية البيانات في القانون الهندي"، المتوفر على: http://idpl.oxfordjournals.org/content/1/1/47.full.pdf+html

المادة رقم 19 (2011)، «جنوب شرق أسيا: حالة التعبير الحر»، متوفر على: http://www.article19.org/resources.php/resource/2258/en/south-east-asia:-the-state-of-free-expression

تشيونج، إيه. (2009)، (.Cheung, A)، "الإنترنت في الصين يشهد حالة ذعر: السعي وراء الإنترنت مقابل حماية السرية"، متوفر على: http://www.sciencedirect.com/science/article/pii/S026736490900065X

فو، واي. لاو، تي.، أتكين، دي. لين، سي. (2011)، (.Wu, Y., Lau, T., Atkin, D. and Lin, C)، "دراسة شاملة للتنظيمات المتعلقة بالسرية على الإنترنت في الولايات المتحدة الأمريكية والصين"، سياسة الاتصالات، الرقم الدولي المتسلسل 5961–0308، 2011، العدد رقم 35، الإصدار رقم 7، الصفحة رقم 603–616.

فاينر، إن. (2007)، (.Viner, N)، "قانون الحريات العالمي على الإنترنت: هل تستطيع شركات الإنترنت الأمريكية تصعيد الجدار الناري الصيني العظيم أمام أبواب القرن الصيني؟"، استعراض قانون ولاية أيوا؛ 2007/1/11، العدد 93 – إصدار رقم 1، ص. 361–391.

بامان، دي.، وأوكونور، ب.، وسميث، إن. (2011)، (.Bamman, D., O›Connor, B. and Smith, N)، "الرقابة وإلقاء الممارسات في شبكات التواصل الاجتماعي الصينية، الاثنين الأول (فرست مانداي)، العدد 17، رقم 3، متوفر على: http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3943/3169

دايبرت، آر. (2001)، (.Deibert, R)، "الضيوف الغامضين والجدران النارية العظيمة: سياسة الأمن الصينية على الإنترنت،" جريدة الاصدارات الاجتماعية، 58، 1:143–158

دايبرت، آر. (2006)، (.Deibert, R)، "عالم الإنترنت الافتراضي الآسيوي للسياسة الجغرافية"، لمحة عن اقتصاديات الشرق الأقصى، متوفر على: http://www.feer.com/articles1/2006/0612/free/p022.html

دايبرت، آر.، وبالفري، جيه.، وروزينيسكي، آر.، وزيتراين، جيه.، (,Deibert, R., Palfrey, J., Rohozinski R. and Zittrain, J.)، (2011)، "الوصول المتحفظ للبيانات: أمن النظام، والهوية، والمقاومة في العالم الإنترنت الافتراضي في آسيا"، قانون الإنترنت – هارفارد، متوفر على: http://oni-access.net/contested/

جرينليف، جي. (2011)، (Greenleaf , G)، "الاستعانة بمصادر خارجية وقانون السرية الجديد بالهند: لا توجد أسباب للذعر" قوانين السرية والتقرير الدولي للأعمال، الإصدار رقم 111، 16–17 أبريل/ نيسان 2011

جرينليف، جي. (2011)، (Greenleaf , G سي)، "إخطار بالمخالفات ونشر التعزيز وتوزيعه في قانون حماية البيانات التايواني DP"، قوانين السرية والتقرير الدولي للأعمال، إصدار رقم 109، 12–13، فبراير/ شباط 2011

جرينليف، جي. (2011)، (Greenleaf , G إيه)، "الهند تحاول حماية البيانات من خلال وضع التنظيمات والقوانين واللوائح المنظمة لها"، قوانين السرية والتقرير الدولي للأعمال، إصدار رقم 110، أبريل/ نيسان 2011

مبادرة الإنترنت المفتوح (2005)، «تصفية الإنترنت في بورما عام 2005: دراسة عن الدولة»، متوفر على: http://opennet.net/studies/burma

مبادرة الإنترنت المفتوح (2005)، «تصفية الإنترنت في الصين عام 2005: دراسة عن الدولة»، متوفر على: http://opennet.net/studies/china

مبادرة الإنترنت المفتوح (2005)، «تصفية الإنترنت في سنغافورة عام 2005: دراسة عن الدولة»، متوفر على:
http://opennet.net/studies/singapore

مبادرة الإنترنت المفتوح (2005)، «تصفية الإنترنت في تونس عام 2005: دراسة عن الدولة» متوفر على:
http://opennet.net/studies/tunisia

مبادرة الإنترنت المفتوح (2006)، «تصفية الإنترنت في فيتنام عامي 2005–2006: دراسة عن الدولة»، متوفر على: http://opennet.net/studies/vietnam

روزينيسكي، آر. (1999)، (Rohozinski, R.)، "وضع خريطة تفصيلية بعالم الإنترنت الروسي: أفاق واتجاهات عن الديمقراطية والإنترنت" (PDF)، ورقة مناقشة UNRISD رقم 115

روزينيسكي، آر. (2000)، (Rohozinski, R.)، "كيف لم يقم الإنترنت بتحويل روسيا"، التاريخ المعاصر، العدد 99، رقم 334

6.5 أمريكا اللاتينية ودول الكاريبي

بيرتوني، إي. (2012)، (Bertoni, E.)، "نحو إنترنت خالٍ من الرقابة. مقترحات من أجل أمريكا اللاتينية"، جامعة باليرمو، وكلية الحقوق، ومركز الدراسات المتعلقة بحرية التعبير والوصول للبيانات والمعلومات، متوفر على: http://www.palermo.edu/cele/english/publication.html

ريمولينا، إن. (2010)، (Remolina, N.)، "هل كولومبيا لديها مستوى كافٍ من الحماية للبيانات الشخصية بما يتلاءم مع المعايير الأوروبية؟"، القانون الدولي، جريدة القانون الدولي الكولومبية، العدد 16 (2010)، صفحة رقم 493

ليوناردي، إم. (2005)، (Leonardi, M.)، "المسئولية المدنية عن الإمداد بالخدمات الخاصة بالإنترنت"، رسالة دكتوراه قام بنشرها الباحث خواريز دي أوليفيرا، 2005، ساو باولو.

ألبورنوز، ب.، وباريندیلي، إف.، وكاباليرو، جيه.، ودواتسو، آر.، وإيسكويفيل، دبليو. (2011)، (Albornoz, B., Barindelli, F., Caballero, J., Duaso, R., and Esquivel, W.)، "حركة الحقوق والعدل الاجتماعي على شبكة الإنترنت" – معهد البحوث القانونية، إيه.آر.، متوفر على: http://hdl.handle.net/10625/46335

باريندیلي، إف. وجريجوريو، سي. (2010)، (Barindelli, F, and Gregorio, C.)، "البيانات الشخصية وحرية التعبير في شبكات التواصل الاجتماعي الرقمية: مذكرة مونتفيديو"، من أجل هذا الغرض، بوينوس آيريز، آيه.آر.، متوفر على: http://hdl.handle.net/10625/46022

بوسيو مونتيز دي أوكا، جيه. (2009)، (Bossio Montes de Oca, J,)، "بيرو: معركة السيطرة على الإنترنت"، اتحاد الاتصالات التقدمية، كويتو، إي.سي.، متوفر على: http://hdl.handle.net/10625/42792

كارفالو ليما، سي.سي. & لايتي مونتيرو، آر. (2011)، (Carvalho Lima, C.C. & Leite Monteiro, R.)/ ملاحظات على مشروع قانون حماية البيانات الشخصية (ملاحظات على مشروع قانون حماية البيانات البرازيلي الجديد)، مراقبة الإنترنت، المرصد الرقمي البرازيلي للسياسات الرقمية البرازيلية، متوفر على: http://securitybreaches.files.wordpress.com/2011/05/anteprojeto-de-lei-brasileiro-sobre-protecao-de-dados-pessoais.pdf

جريجوريو، سي.، وأورنيلاس، إل. (2011)، (Gregorio, C. and Ornelas, L.)، "حماية البيانات الشخصية على شبكات التواصل الاجتماعي الرقمية: لاسيما للأطفال والكبار؛ مذكرة مونتيفيديو"، معهد البحوث القانونية والعدلية، بوينوس آيريز، متوفر على: http://hdl.handle.net/10625/46963

جريجوريو، سي.جي. (2004)، (Gregorio, C.G.)، "حماية البيانات الشخصية: أوروبا والولايات المتحدة الأمريكية، معضلة كبيرة لأمريكا اللاتينية"، متوفر على: http://www.bibliojuridica.org/libros/3/1407/12.pdf

معهد البحوث القانونية والعدلية (2004)، «الإنترنت، والسرية، والنظام القضائي في أمريكا اللاتينية ودول الكاريبي»، آي.آي.جيه.، بوينوس آيريز، إيه.آر.، متوفر على: http://idl-bnc.idrc.ca/dspace/handle/10625/25922

مونتيرو، آر.، ولورانت، سي. (2001)، (Monteiro, R and Laurant, C.)، "مشروع قانون حماية البيانات البرازيلي الجديد يتبنى نظام الإخطار بأي مخالفات تتعلق بالبيانات"، متوفر على: http://blog.security-breaches.com/2011/05/09/new_brazilian_data_protection_bill_adopts_data_breach_notification_regime/

أو. إيه. إس. (2010)، «المبادئ البرلمانية والتوصيات الخاصة بحماية البيانات»، متوفر على: http://thepublicvoice.org/documents/Study_on_Data_Protection-CP25337E04-Eng.pdf

السرية الدولية (2011)، «دليل السرية للناطقين باللغة الإسبانية»، متوفر على: https://www.privacyinternational.org/reports/una-guia-de-privacidad-para-hispanohablantes

رودريجيز، كيه.، (2011)، (Rodriguez, K.)، "سياسة المراقبة: التعدي على السرية في أمريكا اللاتينية"، متوفر على: http://advocacy.globalvoicesonline.org/2011/07/27/the-politics-of-surveillance-the-erosion-of-privacy-in-latin-america/

6.6. أوروبا وأمريكا الشمالية

كارتر، إي. (2005)، (Carter, E.)، "خطاب غير قانوني عن الإنترنت: دراسة الرابط بين الخصائص والسمات الفريدة للإعلام الرقمي والدعاوى القضائية الخاصة بالتشهير"، صحيفة قانون الحاسب الآلي والتكنولوجيا في سانتا كلارا – العدد رقم 21، 2 (يناير/ كانون الثاني 2005): 289-318، متوفر على: http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1376&context=chtlj

إلوود، إس.، وليزاينيسكي، إيه. (2010)، (Elwood, S. and Leszczynski)، السرية، وإعادة ترتيب الأوضاع الخاصة بها: تعهدات جديدة، وممارسات خاصة بالبيانات، ومواقع إنترنت حسب الجغرافيا، جامعة واشنطن، متوفر على: http://www.sciencedirect.com/science/article/pii/S001671851000093X

لين، إي. (2002)، (Lin, E.)، ترتيب أولويات قواعد السرية: استجابة دستورية تجاه الإنترنت، دورية قانون التكنولوجيا ببركلي، متوفر على: http://www.law.berkeley.edu/journals/btlj/articles/vol17/LIN.pdf

بيرجهاردت، تي.، وبويمي، كيه.، وبوخمان، إي.، وكيولينج، جيه، وسيفريديس إيه. (Burghardt, T., Böhm, K., Buchmann, E., Kühling, J. and Sivridis A.)، (2009)، دراسة عن نقص إعمال قوانين حماية البيانات، متوفر على: http://www.law.berkeley.edu/journals/btlj/articles/vol17/LIN.pdf

بيرجهاردت، تي.، وبويمي، كيه.، وبوخمان، إي.، وكيولينج، جيه، وسيفريديس إيه. (Burghardt, T., Böhm, K., Buchmann, E., Kühling, J. and Sivridis A.)، (2009)، دراسة عن نقص إعمال قوانين حماية البيانات، متوفر على: http://dbis.ipd.uni-karlsruhe.de/download/bu09edemocracy.pdf

كوان أون، دبليو.، وميلارد، سي.، ووالدين، آي. (Kuan Hon, W., Millard, C. and Walden)،(2011))، "مشكلة (البيانات الشخصية) في أجهزة خوادم الحفظ الاحتياطية على شبكة الإنترنت: ما هي البيانات الخاضعة للتنظيم والقانون؟ - أجهزة الحفظ في المجهول"، طباعة جامعة أكسفورد، متوفر على: http://idpl.oxfordjournals.org/content/1/4/211.full

موقع now.org، الحقوق الرقمية الأوروبية، الحوار مع المستهلك عبر الأطلسي (2012)، ماذا يجعل ACTA مثيرة للجدل؟ (ولأن البرلمانيين في الاتحاد الأوروبي ينبغي أن يولوا اهتماماً أكبر)، متوفر على: http://www.manzanamecanica.org/files/ACCESS_EDRI_TACD-por_que_oponerse_al_acta_ES.pdf

مجموعة (La Quadrature Du Net) - لاكوادراتيور دي نيت – المختصة بالنشاط الحقوقي والحريات الرقمية على شبكة الإنترنت، الإنترنت والحريات (2012)، تحقيق الفوز في ACTA وما بعدها! متوفر على: http://www.laquadrature.net/en/winning-big-on-acta-and-beyond

اتحاد الحريات المدنية الأمريكية (2011)، الطلبات الحكومية لمستخدمي تطبيق تويتر على الإنترنت، البيانات والمعلومات الشخصية تثير مخاوف دستورية جادة، يقول ACLU، متوفر على: http://www.aclu.org/technology-and-liberty/government-requests-twitter-users-personal-information-raise-serious-constitu

بوديش، آر. (Budish, R.)، (2007)، في مواجهة الخطر: الاعتراف السطحي وحدود قوانين السرية، متوفر على: http://hlr.rubystudio.com/media/pdf/facial_recognition_privacy_law.pdf

مجلس الاتحاد الأوروبي (2011)، الاتفاقية التجارية لمكافحة التزوير (ACTA)، متوفر على:

باللغة الإسبانية:

http://register.consilium.europa.eu/pdf/es/11/st12/st12196.es11.pdf

باللغة الإنجليزية:

http://register.consilium.europa.eu/pdf/en/11/st12/st12196.en11.pdf

دو جوشت، كيه. (De Gucht, K)، (2012)، ACTA: "الاختيار الصحيح"، البرلمان الأوروبي، لجنة التجارة الدولية، متوفر على: http://trade.ec.europa.eu/doclib/docs/2012/june/tradoc_149559.pdf

المفوضية الأوروبية (2010)، «بيان السرية، المشورة العامة بشأن مراجعة نظام الأفضلية طبقاً للتعميم الصادر بشأنها (GSP)" متوفر على: http://trade.ec.europa.eu/doclib/docs/2010/march/tradoc_145976.pdf

جيندين، إس. (1997) ،(Gindin, S.)، الفقدان والظهور بعالم الإنترنت، مقالة عن قانون سان دييجو، متوفر على: http://www.info-law.com/lost.html

المعهد القومي لتكنولوجيا الاتصالات والهيئة الإسبانية لحماية البيانات الشخصية (2009)، «دراسة عن سرية البيانات الشخصية وأمن المعلومات الخاصة بشبكات التواصل الاجتماعي على شبكة الإنترنت»، متوفر على: http://www.inteco.es/Seguridad/Observatorio/Estudios/est_red_sociales_es

LRDP كانتور ومركز الإصلاح العام (2010)، "دراسة مقارنة عن الاتجاهات المختلفة للتحديات الجديدة لنظام سرية المعلومات، لاسيما في ضوء التطورات التكنولوجيا – التقرير النهائي للمفوضية الأوروبية"، متوفر على: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

ميترانو، تي. (2006) ،(Mitrano, T.)، عالم أوسع: الشباب والسرية وتكنولوجيا التواصل الاجتماعي، مقالة EDUCAUSE، المجلد رقم 41، رقم 6، متوفر على: http://www.educause.edu/ero/article/wider-world-youth-privacy-and-social-networking-technologies

بيريز، جيه.سي. (2009) ،(Perez, J.C.)، سيقوم موقع الفيس بوك بغلق بيكون لتسوية الدعوى المرفوعة، نيويورك تايمز، 19 سبتمبر/ أيلول، 2000، متوفر على: http://www.nytimes.com/external/idg/2009/09/19/19idg-facebook-will-shut-down-beacon-to-settle-lawsuit-53916.html

إصدار صحفي/ مذكرة للنشر، مقالة عن مرجعية المفوضية الأوروبية لـ ACTA لمحكمة العدل الأوروبية، متوفر على: http://trade.ec.europa.eu/doclib/docs/2012/may/tradoc_149464.doc.pdf

السرية الدولية (2011) «مراقبة الرقابة 2011: تقييم الرقابة في كل أنحاء أوروبا»، متوفر على: https://www.privacyinternational.org/reports/surveillance-monitor-2011-assessment-of-surveillance-across-europe

دار حقوق السرية، «السرية الرقمية: استخدام الإنترنت بصورة آمنة»، متوفر على: http://www.privacyrights.org/fs/fs18-cyb.htm

سالزمان، في. (2000) ،(Slazmann, V.)، " هل السجلات العامة علنية بالفعل؟ التصادم بين الحق في السرية وإصدار سجلات المحاكم العامة على الإنترنت"، مقالة عن قانون بايلور، متوفر على: http://works.bepress.com/cgi/viewcontent.cgi?article=1011&context=victoria_salzmann

سبراج، آر. (2009) ،(Sprague, R.)، إعادة التفكير في سرية البيانات في عصر الشفافية الرقمية، متوفر على: http://lawarchive.hofstra.edu/pdf/academics/journals/laborandemploymentlawjournal/labor_vol25no2_sprague.pdf

يورك، جيه. سي. (2011) ،(York, J.C.)، قضية الأسماء المستعارة على الإنترنت، متوفر على: https://www.eff.org/deeplinks/2011/07/case-pseudonyms

6.7. نوع الجنس

ألين، إيه. (2000) ،(Allen, A.)، الجنس والسرية في عالم الإنترنت، مقالة بشأن قانون ستانفورد، المجلد رقم 52، العدد 5، ندوة: الإنترنت والسرية: معيار قانوني جديد؟ (مايو، 2000)، صفحة رقم 1175–1200، متوفر على: http://www.jstor.org/stable/1229512

اتحاد الاتصالات التقدمية (2012)، «غياب حرج: النساء في الحوكمة الخاصة بالإنترنت. أدوات الدفاع عن السياسات»، متوفر على: http://www.violenceisnotourculture.org/resources/critically-absent-women-internet-governance-policy-advocacy-toolkit

بارتاو، إيه. (2000) ،(Bartow, A.)، "البيانات الخاصة بنا، والمملوكة لنا: السرية، وتقنين البيانات المملوكة، والجنس"، متوفر على: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=374101

بورنيت، كيه.، وسوبرامانيام، إم.، وجيبسون، إيه. (,(Burnett, K., Subramaniam, M., and Gibson, A 2009))، "اللاتينيات عبر حدود تكنولوجيا المعلومات: فهم الجنس باعتباره موضوع هامشي بين عام المعلومات"، أول يوم اثنين، المجلد رقم 14، العدد رقم 9، متوفر على: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2581/228

كليفورد، بي. (2008) ،(Clifford, B.)، "الحساسية الخاصة بالسرية الرقمية والجنس: حالة عملية عن السكان الناضجين من ذوي التعليم العالي"، متوفر على: http://gradworks.umi.com/33/36/3336862.html

EPIC، "الجنس والسرية الإلكترونية"، متاح على البريد الإلكتروني"، متوفر على: http://epic.org/privacy/gender/

جرابس هوي، إم.، وميلني، جي. (2010) ،(Grubbs Hoy, M. and Milne, G.)، "الفروق والاختلافات الجنسية في المقاييس والإجراءات المتعلقة بالسرية بالنسبة لمستخدمي الفيس بوك من الشباب الكبار". متوفر على: http://jiad.org/article130

2010) VAW)، "السرية الخاصة بك، وسلامتك"، التعدي على المصادر الرقمية الخاصة بالمرأة، متوفر على: http://www.vaw.umn.edu/documents/internet-safety/internet-safety.html

يون، إس.، وهوال، كيه. (2008) ،(Youn, S. and Hall, K.,)، "سرية الجنس والمعلومات الرقمية فيما بين المراهقين: إدراك المخاطر، والمخاوف الخاصة بالسرية، وسلوكيات الحماية"، متوفر على: http://www.ncbi.nlm.nih.gov/pubmed/18954276

قائمة المراجع

التحالف الإقليمي من أجل حرية التعبير والمعلومات، صابر ماس الثالث: التقرير الإقليمي بشأن الحصول على المعلومات وحماية البيانات الشخصية (2011: التحالف الإقليمي من أجل حرية التعبير والمعلومات).

أليسون، دي. (Allison, D)، حماية حقوق الإنسان في العصر الرقمي: فهم تطور حرية التعبير ومخاطر الخصوصية في صناعة تكنولوجيا المعلومات والاتصالات (2011: أعمال عالم أفضل (BSR).

أنج، بي (Ang, P)، "التنظيم الذاتي للخصوصية والإنترنت" (2011) 1 صحيفة الإعلانات التفاعلية 1.

أنجوان، جيه وفالنتينو-ديفريز، جيه (2011)، (Angwin, J., & Valentino-Devries). أي فون أبل وأندرويد جوجل ترسل موقع الهواتف المحمولة. صحيفة وول استريت، تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011، من خلال هذا الرابط: http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html

المادة 19، تعليقات مكتوبة في قضية رقم 524 12 في محكمة البلدان الأمريكية للحقوق الإنسان: جورجي فونتفيشيا

وهيكتور داأميكو (Jorge Fontevecchia and Hector D'amico) الأرجنتين (2011: مادة 19، لندن).

بيكر وماكنزي (Baker & MacKenzie)، " عام كبير للخصوصية في الصين العظمى: نهاية 2011" النشرة الإخبارية: يناير/ كانون الثاني 2012.

بانويل، إل وراي، كيه وكولسون، جي وأوركهات، سي ولونسدال، أر وارمسترونغ، سي وتوماس، أر وآخرون Banwell, L., Ray, K., Coulson, G., Urquhart, C., Lonsdale, R., Armstrong, C., Thomas, R., et al)،(2004)). إطار رصد وتقييم سلوك المستخدم للجنة المشتركة لأنظمة المعلومات. صحيفة الوثائق 60(3), 302-320.

بيريسفورد، إيه واستاجانو إف. (2003)، (Beresford A. and Stajano F) "خصوصية الموقع في الحوسبة المتغلغلة"، مؤسسة الاتصالات معهد المهندسين الكهربائيين والالكترونيين (IEEE)

http://www.cl.cam.ac.uk/~fms27/papers/2003-BeresfordSta-location.pdf

بيرمان، كاي (2011)، (Biermann, Kai). «حماية البيانات: الإفشاء من خلال البيانات الخاصة بنا.» ZWIT عبر الإنترنت. تم الاسترجاع بتاريخ 1 مارس/ آذار 2012

(http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz)

بتات الحرية، مساهمة بتات الحرية (Bits of Freedom) المراجعة المرحلية الدولية الثناية لهولندا من خلال مجلس الأمم المتحدة لحقوق الإنسان (2011: بتات الحرية، أمستردام).

بلوستن، إي (Bloustein, E) "الخصوصية كجانب للكرامة الإنسانية: الرد على عميد بروسر (1964)، استعراض قانون جامعة نيويورك.962

بويد، دي وهارجيتيا، إي وشولتز، جيه و بالفري جيه (,Boyd, D., Hargittai, E., Schultz, J., & Palfrey 2011) ،(J). لماذا يساعد الآباء أبنائهم في الكذب على الفيس بوك بشأن العمر: عواقب غير مقصودة "لقانون حماية خصوصية الأطفال على الإنترنت" فرست مانداي 16، (11).

برنتون، إم ((Brenton, M، (1964) غزاة الخصوصية، كاورد- ماكان (Coward-McCann).

بلتويز، (2011) ،(BuiltWith) احصائيات الاستخدام التحليلي لجوجل - المواقع الإلكترونية التي تستخدم تحليلات جوجل. تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2012، متوافر من خلال: http://trends. builtwith.com/analytics/Google-Analytics

بورشل، جيه (Burchell, J)، "الحماية القانونية للخصوصية في جنوب إفريقيا: الهجين الذي من الممكن زراعته" (2009) 13الصحيفة الإلكترونية من القانون المقارن 1.

كابانيلاس، جي ((Cabanellas, G، "الحق في الدعاية وفقاً لقانون الأرجنتين" (1998) 18 مراجعة قانون الترفيه بجامعة لويولا بلوس أنجلوس 449.

كاي، إل و شين،إتش. ((Cai, L., & Chen, H، (2011) تاتش لوجر (TouchLogger) الاستدلال على ضربات المفاتيح على الشاشة التي تعمل باللمس من حركة الهاتف الذكي. إجراء 11 للقسم الساخن من مؤتمر (اتحاد الحوسبة التقنية المتقدمة) USENIX السادس بشأن الموضوعات الساخنة في مجال الأمن (صفحة 9) بيركلي، كاليفورنيا، الولايات المتحدة الأمريكية: رابطة اتحاد الحوسبة التقنية المتقدمة USENIX.

كالكوت، دي وآخرون، (1990) ،(Calcutt, D., et al). تقرير اللجنة بشأن الخصوصية والموضوعات ذات الصلة، رئيس مجلس الإدارة السيد/ ديفيد كالكوت (David Calcutt QC)، لندن: مكتب قرطاسية جلالتها (HMSO)، (Cmnd. 1102).

كاراسكولا، إل، (Carrasquilla, L)، (حماية البيانات الشخصية في أمريكا اللاتينية: الاحتفاظ بالبيانات الشخصية ومعالجتها في مجال الإنترنت"، في بيرتوني، إي، إي دي. (Bertoni, E., Ed). نحو إنترنت محرر من الرقابة. المقترحات الخاصة بأمريكا اللاتينية (2012، مركز الدراسات المعني بحرية التعبير والحصول على المعلومات (CELE)، بوينس آيرس)، (Buenos Aires).

كارتر، دي. إل. وكارتر، جيه. سي. (2009) ،(Carter, D. L., & Carter, J. G) عملية تبادل المعلومات الاستخباراتية لتعزيز قانون الدولة والقانون المحلي والقبلي. العدالة الجنائية والسلوك، 36(12), 1323-1339.

كافوكيان، إيه. «تصوير الجسم بالكامل في أجهزة الماسحات الضوئية في المطارات: البناء في الخصوصية من خلال التصميم» مفوض المعلومات والخصوصية، أونتاريو، كندا. يوينو 2009. متاح من خلال هذا الرابط:

http://www.ipc.on.ca/images/Resources/wholebodyimaging.pdf

مركز الديمقراطية والتكنولوجيا، أوامر رسمية للاحتفاظ بالبيانات: تهديد للخصوصية وحرية التعبير وتطوير الأعمال (2011: مركز الديمقراطية والتكنولوجيا، واشنطن)

مركز الديمقراطية والتكنولوجيا، الرؤية دليل التعريف: تقنية التعرف من خلال الوجه الخصوصية ((Seeing Is ID' ing، (2011: مركز الديمقراطية والتكنولوجيا، واشنطن).

نادي شاوس للكمبيوتر. (2011). نادي شاوس للكمبيوتر يحلل البرمجيات الحكومية الخبيثة. تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011، متوافر من خلال هذا الرابط: http://ccc.de/en/ updates/2011/staatstrojaner

تشو، دي. (Cho, D)، قانون التحقق من الاسم الحقيقي على شبكة الإنترنت: هل هو سم أم علاج للخصوصية؟ متاح من خلال هذا الرابط: http://weis2011.econinfosec.org/papers/Real%20Name%20Verification%20Law%20on%20the%20Internet%20-%20A%20Poison%20or%20Cu.pdf

سيريو، بي و وودوفيكو، إيه (2011)، (Cirio, P., & Ludovico, A). وجهاً للفيس بوك. وجهاً للفيس بوك. تم الاسترجاع من خلال هذا الموقع: www.face-to-facebook.net/theory.php

كلارك، جي. (2011). لا تتعقب القوانين لكسب الزخم الأمريكي. السجل (ريجستر). تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011 من خلال هذا الرابط: http://www.theregister.co.uk/2011/05/06/senate_do_not_track/

كومبا، إي. وبيرتوني، إي. (Compa, E. and Bertoni, E)، الأنماط البارزة في حرية التعبير عبر الإنترنت: نتائج البحث المقارن في الأرجنتين والخارج (2010: مركز الدراسات المعني بحرية التعبير والحصول على المعلومات (CELE)، بوينس آيرس)، (Buenos Aires).

كوبر، إيه. (2007)، (Cooper, A). التنافس بشأن الخصوصية. مركز الديمقراطية والتكنولوجيا. تم الاسترجاع بتاريخ: 13 ديسمبر/ كانون الأول 2011 من خلال هذا الرابط: https://www.cdt.org/blogs/alissa-cooper/competing-privacy

الإيكونوميست، (2010) "النقر للذهب: كيف تستفيد شركات الإنترنت من البيانات الموجودة على المواقع الإلكترونية"، في "طريق خاص بشأن إدارة المعلومات" الإيكونوميست، مجلد 394، عدد 8671

إيدلمان، بي. (2006)، (Edelman, B)، "سوء الاختيار عبر الإنترنت" "شهادات الثقة" كلية الأعمال بجامعة هارفارد، تم النشر على شبكة الإنترنت من خلال هذا الموقع: http://www.benedelman.org/publications/advsel-trust.pdf

مؤسسة الحدود الإلكترونية (2011) .(EFF). أجهزة الهواتف المحمولة. مشروع الدفاع الذاتي عن المراقبة. تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011 من خلال هذا الرابط: https://ssd.eff.org/tech/mobile

مركز معلومات الخصوصية الإلكترونية والمنظمة الدولية لحماية الخصوصية والخصوصية وحقوق الإنسان 2006: دراسة مسحية دولية لقوانين وتطورات الخصوصية (مركز معلومات الخصوصية الإلكترونية والمنظمة الدولية لحماية الخصوصية، الولايات المتحدة الأمريكية).

مركز معلومات الخصوصية الإلكترونية. (2011). تقنية التعرف عن طريق الوجه. (EPIC)، تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011 من خلال هذا الرابط: https://epic.org/privacy/facerecognition/

مركز معلومات الخصوصية الإلكترونية. (2011). تقنيات المراقبة الشخصية، تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011 من خلال هذا الرابط: https://epic.org/privacy/dv/personal_surveillance.html

مركز معلومات الخصوصية الإلكترونية. (2011). خصوصية الشبكات الاجتماعية. تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011 من خلال هذا الرابط: https://epic.org/privacy/socialnet/

إندرز، إيه. وهانجنبرج، إتش. ودينكر، إتش. وبي. وموش، إس. (Enders, A., Hungenberg, H., Denker, H.–P., & Mauch, S.)، (2008). الذيل الطويل للشبكات الاجتماعية. نماذج إيرادات مواقع الشبكات الاجتماعية. صحيفة الإدارة الأوربية، 26 (3).

مركز معلومات الخصوصية الإلكترونية (EPIC)، الحوسبة السحابية، تم النشر على الإنترنت من خلال هذا الرابط: http://epic.org/privacy/cloudcomputing/

مركز معلومات الخصوصية الإلكترونية (WHOIS ،EPIC)، تم النشر على الإنترنت من خلال هذا الرابط: http://epic.org/privacy/whois/

مركز معلومات الخصوصية الإلكترونية (EPIC)، رسم صورة للخصوصية والمستهلك، http://epic.org/privacy/profiling/

اللجنة الأوربية، تقرير صادر عن اللجنة للمجلس والبرلمان الأوربي: تقرير التقييم بشأن توجيهات الاحتفاظ بالبيانات (التوجيه EC/24/2006)، بروكسل، 18 أبريل/ نيسان 2011، 225 (2011) com نهائي.

المفوضية الأوربية. (2010). الأجندة الرقمية: تحيل المفوضية المملكة المتحدة إلي المحكمة بشأن الخصوصية وحماية البيانات الشخصية [IP/10/1215]، تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011 من خلال هذا الرابط: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1215

الحقوق الرقمية الأوربية (EDRI) تقرير تقييم الظل بشان توجيه الاحتفاظ بالبيانات (EC 2006/24/17) أبريل/ نيسان 2011: الحقوق الرقمية الأوربية، بركسل).

البرلمان الأوربي. (2000). ميثاق الاتحاد الأوربي للحقوق الأساسية، لوكسمبورج: مكتب المنشورات الرسمية للمجتمعات الأوربية.

فيس بوك، (2012)"احصائيات" تم النشر على الإنترنت من خلال: http://www.facebook.com/press/info.php?statistics

فياض، يو. وغرينشتاين، جي. وويرس، إيه. (2001)، (Fayyad, U., Grinstein, G. and Wierse, A) «تصور المعلومات في استخراج البيانات واكتشاف المعرفة» الناشر مرجان كوفمان.

لجنة التجارة الفيدرالية، (1999) "التنظيم الذاتي والخصوصية عبر الإنترنت: تقرير إلي الكونجرس" مارس/ آذار 1999، تم النشر على الإنترنت على الموقع الإلكتروني: http://www.ftc.gov/os/1999/07/privacy99.pdf

لجنة التجارة الفيدرالية، حماية خصوصية المستهلك في عصر التغيير السريع: إطار العمل المقترح للشركات وصانعي السياسات: التقرير المبدئي للعاملين في لجنة التجارة الفيدرالية، ديسمبر/ كانون الأول 2010.

فرنانديز، جي. (Fernández, G) تنشر الصين مسودة المبادئ التوجيهية للخصوصية، 14 أبريل/ نيسان 2011، هوجان لافلس (Hogan Lovells).

فيلاستو،إيه. (2011) ،(Filastò, A). سجلات أجهزة المعطف الأزرق (Blue Coat) تشير إلي مستويات الرقابة في سوريا. تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011، من خلال http://hellais.github.com/syria-censorship/

فيليبي، بي. دي. (2011) ،(Filippi, P. de). ملاحظات بشأن الخصوصية في السحابة.

فيتزباتريك، إم. (Fitzpatrick, M) "الهاتف المحمول الذي يسمح لأرباب العمل بالتجسس على الموظفين" بي بي سي نيوز 10/03/2010، متوافر من خلال:

http://news.bbc.co.uk/1/hi/technology/8559683.stm

فلاهرتي، دي. إتش. (1999)، (Flaherty, D. H) رؤى حول الخصوصية:الماضي والحاضر والمستقبل. رؤى حول الخصوصية: خيارات السياسات بالنسبة للعصر الرقمي (ص. 19–38). دار نشر جامعة تورونتو برس.

فوكس، سي. (2009)، (Fuchs, C). مواقع الشبكات الاجتماعية ومجتمع المراقبة. دراسة نقدية لحالة استخدام استوديفز (studiVZ) والفيس بوك(Facebook) وماي سبيس (MySapace) بواسطة الطلاب في سالزبورغ في سياق المراقبة الإلكترونية. سالزبورغ: فورتشنجسجروب (Forschungsgruppe) "النظرية الموحدة للمعلومات"

غيتس، جيه. (Gates, J) والمجموعة العاملة في الخصوصية. (1995). الخصوصية والبنية التحتية الوطنية للمعلومات: المبادىء الخاصة بتوفير المعلومات الشخصية واستخدامها. لجنة سياسة المعلومات، قوة مهمة البنية التحتية للمعلومات، متاح من خلال: http://aspe.hhs.gov/datacncl/niiprivp.htm

جلمان، أر. (Gellman, R) والمنتدى العالمي للخصوصية. (2009). الخصوصية في السحب: مخاطر الخصوصية والسرية من حوسبة السحابية، تم الاسترجاع من خلال: http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

جوجل ((Google. (2008) جوجل روح العصر 2008. تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011، من خلال: https://www.google.com/intl/en/press/zeitgeist2008/world.html#top

جوجل ((2011) (Google تقرير الشفافية الخاص بجوجل. جوجل. تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011، من خلال: https://www.google.com/transparencyreport/

جورج، إم. (2008) (Gorge, M.). حماية البيانات: لماذا لا تزال المنظمات غير مدركة للفكرة الصحيحة؟ الاحتيال الحاسوبي والأمن، معرف الوثيقة الإلكترونية: 10.1016/S1361–3723(08)70095–2 2008 (6)، 5–8.

جرين ليف، جي. (Greenleaf, G) "آسيا – خصوصية البيانات في دول الباسيفيك: 2011، عام الثورة؟" UNSWLRS 30 [2011]

جرين ليف، جي. (Greenleaf, G)، تأثير معايير خصوصية البيانات خارج أوربا: الآثار المترتبة على عولمة اتفاقية 108، جامعة نيو ساوث ويلز، كلية سلاسل أبحاث القانون، ورقة 42، 2011

غريفيث، جيه (Griffiths, J)، (بدون تاريخ) سلوك بحث الطلاب وشبكة الإنترنت: استخدام الموارد الأكاديمية وجوجل. اتجاهات مكتبية، 2005، مجلد 53، رقم 4، ص. 539– 554، http://www

هارجيتاي، إي. (Hargittai, E). الثقة عبر الإنترنت: تقييم الشباب لمحتوى شبكة الإنترنت. الصحيفة الدولية للاتصالات، 4.

هيجينبوثام، إس (2010)، (Higginbotham, S). أجهزة استشعار أي فون فور(iPhone 4) تسلط الضوء على. VCs GigaOM. تم الاسترجاع من خلال:

http://gigaom.com/2010/06/08/iphone-4-sensors-highlight-a-bright-spot-for-vcs/

هلس، إل. وجوجندشوتز نت. (Hilles, L., & Jugendschutz.Net)، (2011). فيرلوكت – فيرلينكت – فيرليرنت؟ ويربنج، فيرنتزونج اوند داتنابفراجن أوف كيندرسيتن – (Verlockt – Verlinkt – verlernt? Werbung, Vernetzung und Datenabfragen auf Kinderseiten) ماينز، ألمانيا.

مجلس حقوق الإنسان (2009)، «تعزيز وحماية كافة حقوق الإنسان، المدنية والسياسية والاقتصادية، والاجتماعية والثقافية، بما في ذلك الحق في التنمية: تقرير المقرر الخاص بشأن تعزيز وحماية حقوق الإنسان والحريات الأساسية في مقابل مكافحة الإرهاب، مارتن شينين" مجلس حقوق الإنسان، الدورة الثالثة عشر، بند 3، بتاريخ 28 ديسمبر/ كانون الأول 2009، A/HRC/13/37

http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf

هنتون وويليامز،(Hunton & Williams) تنبيه العميل، يناير/ كانون الثاني 2010، متاح من خلال:

http://www.hunton.com/files/News/4bfa5361-4d8f-4c7e-af03-75055a82202c/Presentation/NewsAttachment/7d2612ba-40d6-4884-83de-c01965341d41/new_chinese_tort_liability_law.pdf

Initiative Vorratsdatenspeicherung. (2011). Stoppt die Vorratsdatenspeicherung

تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011، من خلال:

https://www.vorratsdatenspeicherung.de/static/verfassungsbeschwerde_de.html

محكمة البلدان الأمريكية لحقوق الإنسان، تقرير حول وضع المدافعين عن حقوق الإنسان في الأمريكتين، متاح من خلال: http://www.cidh.org/countryrep/defenders/defenderschap1-4.htm

إنترونا، إل. دي ونيسنبوم، إتش. إف. (Introna, L. D., & Nissenbaum, H. F) تقنية التعرف من خلال الوجه. مسح لقضايا السياسة والتنفيذ. المكتبة الإلكترونية للرقم الدولي المعياري التسلسلي. معرف الوثيقة الإلكترونية: 10.2139/ssrn.1437730

الاتحاد الدولي للاتصالات (ITU)) الاتصالات العالمية، 2010. قياس مجتمع الإنترنت. (عبر الإنترنت) http://www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010_without_annex_4-e.pdf

كيلكيلي، يو. (Kilkelly, U)، الحق في احترام الحياة الخاصة والحياة العائلية: دليل لتنفيذ المادة 8 من الاتفاقية الأوربية لحقوق الإنسان: كتيبات حقوق الإنسان، رقم 1 (2001: الإدارة العامة للحقوق الإنسان، مجلس أوربا، ستراسبورغ)

كنج، إي (2011) ،(King, E). استجابتنا لمشاورات الاتحاد الأوربي بشأن شرعية المراقبة على التصدير وتقنية الرقابة. المنظمة الدولية لحماية الخصوصية. تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011، من خلال: https://www.privacyinternational.org/article/our-response-eu-consultation-legality-exporting-surveillance-and-censorship-technology

كوبس، بي. وسلويس، جيه. (Koops, B., and Sluijs, J)، حيادة الشبكات والخصوصية وفقاً للمادة 8 المحكمة الدولية للحقوق الإنسان، كلية تيلبورغ للقانون الرقم الدولي المعياري التسلسلي لوثائق الأبحاث الدراسات القانونية: 2011/017

لارو، إف. (La Rue, F)، (2011). تقرير المقرر الخاص بشأن تعزيز وحماية الحق في حرية الرأي والتعبير، فرانك لارو لمجلس الأمم المتحدة لحقوق الإنسان [23/A/HRC/14]. جينف، الأمم المتحدة.

ليون، بي. وأور، بي. وبالباكو، أر. وكارنور، إل. وشاي، أر. ووانغ، واي. (Leon, P., Ur, B., Balebako, R., Cranor, L., Shay, R., and Wang, Y)، لماذا لم يستطع جونى أن يختار الانسحاب: تقييم إمكانية استخدام الأدوات للحد من الدعاية السلوكية (2011: جامعة كارنيجي ميلون، بيتسبرغ).

ليونغ، إف وبكر، إتش (Leong, F. and Bakar, H)، "قانون حماية البيانات الشخصية 2010" (يوليو/ تموز –سبتمبر/ أيلول 2010) هيرالد القانونية 1

ليسيغ، إل. (Lessig, L) "لوائح وقوانين الفضاء الإلكتروني" الكتب الأساسية، نيويورك

مارينوس، إل. (Marinos, L) والوكالة الأوربية لأمن الشبكات والمعلومات. (2011). السلوك التعسفي الإلكتروني والتهيئة عبر الإنترنت: المساعدة في الحماية ضد المخاطر. هيراكليون، اليونان.

مارش، أر. (Marsh, R)، "التشريع الخاص بالتنظيم الذاتي الفعال: نهج جديد لحماية الخصوصية الشخصية على الإنترنت" (2009) 15 مجلة ميشيغان الخاصة بقانون الاتصالات والتكنولوجيا 543.

ماير، جيه. (Mayer, J) تتبع المتتبعين: الإعلان عن ميكروسوفت. مركز الإنترنت والمجتمع (CIS)، كلية ستانفورد للقانون. تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011، من خلال: http://cyberlaw.stanford.edu/node/6715

ماكنزي، بي. ديكر، إيه وفانج، جيه. (McKenzie, P. Dicker, A., and Fang, J) المبادىء التوجيهية الجديدة للصين بشأن جماية خصوصية البيانات، 11 أبريل/ نيسان 2011 (موريسون فورستر) (Morrison Foerster)

ماكنزي، بي وميلنر، جي (McKenzie, P., and Milner, G)، تحديث الصين، مارس/ آذار 2009: أحدث المستجدات في حماية البيانات، 9 مارس/ آذار 2009 (موريسون فورستر) (Morrison Foerster)

ماكنزي، بي وميلنر، جي (McKenzie, P., and Milner, G)، خصوصية البيانات في الصين: تطورات القانون الجنائي، 25 يناير/ كانون الثاني 2010 (موريسون فورستر) (Morrison Foerster)

مولر، إم. (2011) ،(Mueller, M) تقنية الفحص العميق للحزمة DPI)) من وجهة نظر دراسات حوكمة الإنترنت: مقدمة. جامعة سيراكيوز. تم الاسترجاع من خلال: http://dpi.ischool.syr.edu/Technology_files/WhatisDPI-2.pdf

مولر، إم. إل (2010) ،(L..Mueller, M). الشبكات والدول: السيسات العالمية لحوكمة الإنترنت (ص.280). دار نشر إم أي تي برس (MIT Press).

مولر، بي. (Mueller, P)، (2011) Offene Staatskunst – Strategie für eine vernetzte Welt. Arbeitskreis حوكمة الإنترنت. موينخ، ألمانيا: MCG) Münchner Centrum für Governance-Forschung).

بيتر، دبليو. (Netter, W) "موت الخصوصية" وحدة الخصوصية 1: مقدمة لرسم صورة جانبية للبيانات، جامعة هارفارد، 2002

http://cyber.law.harvard.edu/privacy/Module2_Intro.html

نيميتز، في ألمانيا (1992)، 16 EHRR 97

أونج، أر. (Ong, R)، "الاعتراف بالحق في الخصوصية بشأن الإنترنت في الصين" (2011) 1 القانون الدولي للخصوصية البيانات 172.

بادانيا، إس. وغريغوري، يو. وألبردينجك- تيجم، يو. ونونيز، بي (-Padania, S., Gregory, S., Alberdingk Thijm, Y., & Nunez, B) تقرير حول وجود الكاميرات في كل مكان 2011، تم الاسترجاع من خلال: http://www.witness.org/cameras-everywhere/report-2011

بانج، دي. وتشن، بي. ولي، دي. (2008). الثمانية منعقد الآن بشأن مشكلات الجنس على الإنترنت (Eight now held in internet sex probe). المعيار. تم الاسترجاع بتاريخ 31 ديسمبر/ كانون الأول 2011، من خلال:

http://www.thestandard.com.hk/news_detail.asp?pp_cat=12&art_id=61125&sid=17431562&con_type=3#

بومفريت، جيه. (2009) ،(Pomfret, J). فني مدان في قضية اديسون تشن الخاصة بالصور الجنسية. صحيفة فيكتوريا نيوز.

تم الاسترجاع بتاريخ 31 ديسمبر/ كانون الأول 2011، من خلال:

http://www.vicnews.com/entertainment/television/43998412.html

مؤسسة الخصوصية، 9 يوليو/ تموز 2001 http://www.sonic.net/~undoc/extent.htm

المنظمة الدولية لحماية الخصوصية، (2006) "الخصوصية وحقوق الإنسان 2006: دراسة دولية مسحية لقوانين وتطورات الخصوصية»

http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-20Rights%20Human%20and%65435&als[theme]=Privacy

المنظمة الدولية لحماية الخصوصية، 1996، أسئلة يتم طرحها بصورة متكررة حول بطاقة الهوية. https://www.privacyinternational.org/article/id-card-frequently-asked-questions

المنظمة الدولية لحماية الخصوصية، 2006. المنظمة الدولية لحماية الخصوصية، 2006 – ملخص تنفيذي. تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011، من خلال: https://www.privacyinternational.org/article/phr2006-executive-summary

المنظمة الدولية لحماية الخصوصية، (2011). المملكة المتحدة – لمحة حول الخصوصية. المنظمة الدولية لحماية الخصوصية. تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011، من خلال: https://www.privacyinternational.org/article/united-kingdom-privacy-profile

غرفة مقاصة حقوق الخصوصية، (2010)، "صحيفة الوقائع 18: الخصوصية والإنترنت: التنقل في الفضاء الإلكتروني بأمان"، تم النشر على الإنترنت من خلال: http://www.privacyrights.org/fs/fs18-cyb.htm

ريدنج، في. (Reding, V)، الخطوات التالية نحو العدالة والحقوق الأساسية والمواطنة في الاتحاد الأوربي. بيان موجز لمركز السياسة الأوربية، بروكسل 18 مارس/ آذار 2010، بروكسل. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/108

روبرتسون، دي. أس. (1998) ،(Robertson, D. S). النهضة الحديثة: أجهزة الحاسوب والمستوى التالي من الحضارة (ص. 208). دار نشر جامعة أكسفورد، الولايات المتحدة الأمريكية.

روبنسون، إن. وغرو، إتش. وبوترمان، إم. وفاليري، إل. (Robinson, N., Graux, H., Botterman, M., and Valieri, L)، استعراض توجيهات الاتحاد الأوربي بشأن حماية البيانات، ملخص، تم إعداده لمكتب مفوض المعلومات بالمملكة المتحدة، مايو/ أيار 2009

روني، بي. (2011)، (Rooney, B) تنشر المملكة المتحدة المبادىء التوجيهية "Cookie" للاتحاد الأوربي. صحيفة وول ستريت، تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011، من خلال: http://blogs.wsj.com/tech-europe/2011/05/09/u-k-publishes-e-u-cookie-directive-guidelines/

روس، إل. وجاو، كيه. و وتشو، إيه. (Ross, L., Gao, K., and Zhou, A) مسودة المبادىء التوجيهية لقضايا الصين بشأن الخصوصية عبر الإنترنت، تعلن وكالة جديدة للإشراف على الإنترنت، 19 مايو/ أيار 2011 (يلمر هيل).

روتنبرج إم. وهوفناجلم، سي. (Rotenburg M. And Hoofnaglem C) "الامتثال للجنة إصلاح الحكومة بشأن استخراج البيانات" 25 مارس/ آذار 2003. http://epic.org/privacy/profiling/datamining3.25.03.html

شولمان، إيه. (Schulman, A) "مدى الرصد المنهجي لاستخدام الموظف للبريد الإلكتروني والإنترنت"

سكوت، جيه. سي. (Scott, J. C.) (الرؤية تشبه الحالة) seeing like a state: كيف باءت بعض الخطط الرامية إلي تحسين وضع الإنسان بالفشل. نيو هافن: دار نشر جامعة ييل.

سينور، إيه. وبنكانتي، إس. (2011)، (Senior, A., & Pankanti, S). حماية الخصوصية وتقنية التعرف عن طرق الوجه.

In S. Z. Li & A. K. Jain (محررون)، كتيب تقنية التعرف عن طريق الوجه. اسبرنجر.

شاكر، إل. (3)، (Shaker, L.) أبريل/ نيسان 2006). نحن نثق في جوجل: نزاهة المعلومات في العصر الرقمي. فرست مانداي، غوش ريشاب أير. تم الاسترجاع من خلال: http://frodo.lib.uic.edu/ojsjournals/index.php/fm/article/view/1320/1240

سيلفا، إيه. (Silva, A)، "حماية البيانات الشخصية وخدمات الإنترنت في أمريكا اللاتينية" في بيرتوني، إي ((Bertoni, E.، طبعة، نحو إنترنت خالي من الرقابة. مقترحات لأمريكا اللاتينية (2012، مركز الدراسات المعني بحرية التعبير والحصول على المعلومات (CELE)، بوينس آيرس)، (Buenos Aires).

سيلفر، في. والجين، بي. (2011) (Silver, V., & Elgin, B). التعذيب في البحرين يتحول إلي روتين بمساعدة من نوكيا، سيمنز، بلومبرغ. تم الاسترجاع بتاريخ 28 أغسطس/ آب 2011، من خلال: http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html

سوجيان، سي. (2007)، (Soghoian, C.) "مشكلة أبحاث التفاهات غير المعروفة" جامعة إنديانا بلومنجتون – كلية المعلوماتية. تم النشر على الإنترنت من خلال:

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=953673

سولوف، دي. جي. (2008) فهم الخصوصية، دار نشر جامعة هارفارد.

سون، بي وكوكر، إم. (2011). المؤسسات الأجنبية التي ساعدت القذافي في التجسس على الليبيين، صحفية وول استريت، تم الاسترجاع بتاريخ 23 سبتمبر/ أيلول 2011، من خلال:

http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html

لجنة إصلاح قوانين جنوب إفريقيا، مشروع 124: تقرير حول الخصوصية وحماية البيانات (2009: لجنة إصلاح قوانين جنوب إفريقيا)

ستيوارت، بي. (Stewart, B). مسح مقارن لهيئات حماية البيانات. قانون الخصوصية وتقرير السياسات، 11(2).

ستوارت، كيه. (2011)، (Stuart, K) اختراق شبكة بلاي ستيشن: ماذا يحتاج كل مستخدم أن يعرف. صحيفة الجارديان. تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011، من خلال:

http://www.guardian.co.uk/technology/gamesblog/2011/apr/27/psn-security-advice

سونغ- جين، بي. (Sung-jin, Y) (2011). 35 مليون مستخدم لخدمة الشبكة الاجتماعية بكوريا الجنوبية (Cyworld)، حيث تم اختراق شبكة المعلومات في كوريا الجنوبية. كوريا هيرالد. تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011، http://www.koreaherald.com/national/Detail.jsp?newsMLId=20110728000881

سويني، إل. (Sweeney, L) "استراتيجيات عدم تعريف بيانات المريض عند إجراء الأبحاث" جامعة كارنيجي ميلون، مختبر خصوصية البيانات، 1998 http://www.ocri.ca/ehip/2005/presentations/Sweeney_bw.pdf

مركز أبحاث الاتصالات. (2011). الاتصالات العالمية. جينف: الاتحاد الدولي للاتصالات. الايكونوميست، (2010) "قواعد جديدة للبيانات الكبيرة" في "تقرير خاص حول إدارة المعلومات" الايكونوميست، مجلد 394، عدد 8671

ترست (2009)، (TRUSTe)، إصدارات ووقائع دار النشر ترست" تم النشر على الإنترنت من خلال:

http://www.truste.com/about_TRUSTe/press-room.html

توفيكسي، زد. (Tufekci, Z). الفيس بوك: الخصصة في حياتنا الخاصة وفي المدينة المملوكة لشركة معينة. علم الاجتماع التقني. أدواتنا، أنفسنا. تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011، من خلال: http://technosociology.org/?p=131

لجنة الأمم المتحدة لحقوق الإنسان، التعليق العام رقم. 16: الحق في احترام الخصوصية الأسرة والمنزل المراسلات وحماية الشرف والسمعة (مادة 17)، اعتمدت بتاريخ 4 أغسطس/ آب 1988

فالنتينو- ديفريس، جيه. و سون، بي. وملس، إن. ((Valentino-Devries, J., Sonne, P., & Malas, N 2011)). بلوكوت (Blue Coat) تقر باستخدام أجهزتها للرقابة على الإنترنت في سوريا وسط الربيع العربي. صحيفة وول ستريت، تم الاسترجاع بتاريخ 13 ديسمبر/ كانون الأول 2011، من خلال:

http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

فاسيلي، جيه. (2011)، (Vasile, J). تقديم صندوق الحرية (فريدم بوكس). 2010 – الموسيق والفنون والخطاب السياسي. غراتس، النمسا: Verein zur Förderung des gesellschaftspolitischen und kulturellen Austausches.

فوليو، إف. (Volio, F) "الشخصية القانونية، الخصوصية والأسرة" في هانكين (طبعة)، الشرعة القانونية للحقوق الإنسان (دار نشر جامعة كولومبيا 1981).

(W3Techs، 2011). احصائيات الاستخدام وحصة السوق من أدوات تحليل التجارة غير المشروعة للمواقع الإلكترونية. تقدم Q–Success مجموعة من الخدمات من خلال الإنترنت. تم بتاريخ 13 ديسمبر/ كانون الأول 2011، من خلال: http://w3techs.com/technologies/overview/traffic_analysis/all

وارن، اس وبرانديز، إل. (Warren, S. and Brandeis, L) "الحق في الخصوصية" (1890) 4 مجلة قانون هارفارد 193

ويبر، تي (Weber, T) يزداد التهديد بالجريمة الإلكترونية بصورة كبيرة، بي بي سي نيوز، 31/01/09 http://news.bbc.co.uk/1/hi/business/davos/7862549.stm

ويستن، إيه. (1967) (Westin, A) "الخصوصية والحرية" أثينيوم، نيويورك

ورك مان، أر. (Workman, R)، "التوازن بين الحق في الخصوصية والتعديل الأول" (1992) 29 مجلة هوستن القانونية 1059

يورك، جيه. سي. (2010)، (York, J. C.). محتوى السياسات في المجال شبه العام. بوستن، إم إيه: نشرة مبادرة الشبكة المفتوحة. مركز بيركمان. جامعة هارفارد.

المقابلات:

البروفيسور جاو لينج، (Guo Liang)، مدير مشروع الإنترنت في الصين وعضو الفريق الاستشاري لأصحاب المصلحة المتعددين التابع الأمين العام للأمم المتحدة لمنتدى حوكمة الإنترنت، أكاديمية العلوم الاجتماعية، الصين.

السيد/ يانغ وانغ، (Yang Wang) دكتوراه، عالم أبحاث، جامعة كارينجي ميلون، CyLab، الولايات المتحدة الأمريكية

السيدة/ سيرين أونال، إل. إل. إم. (Ceren Unal, LL.M)، قسم القانون المدني، جامعة بيلكنت، كلية الحقوق

البروفيسور أنج بينج هوا، (ANG Peng Hwa) خبير في قانون الإنترنت في سنغافورة، مدير، مركز أبحاث الإنترنت بسنغافورة.

السيد/ إيرك إيريرت أهون، (Erick Iriarte Ahon) خبير الخصوصية في أمريكا اللاتينية، مراقب في أمريكا اللاتينية

كاتيتزا رودريجيز، (Katitza Rodriguez) مدير حقوق الإنسان، EFF

كارين رايلي، ((Karen Reilly مدير السياسة العامة، مشروع TOR

على جي. رافي، تكتيكال (G. Ravi, TacticalTech Ali)

معز شاكشوك،((Moez ChackchouK الجمعية التونسية للإنترنت

بريمافيرا دي فيليبي،((Primavera de Filippi جامعة بانتيون عساس باريس 2

بيتر باريسيك، رئيس مركز الحوكمة الإللكترونية، Donau-Universität Krems

روبرت بودل، يوني مونت جوزيف (Robert Bodle, Uni Mount Joseph)

سمير بادانيا، ماكروسكوب وشاهد (Sameer Padania, Macroscope and Witness)

بيتر برادويل، مجموعة الحقوق المفتوحة

أولريك هوبنر، فولفغانغ غوته (Ulrike Höppner, Johann Wolfgang Goethe) – جامعة فرانكفورت

مجهول، موظف سابق شركة كبيرة للتكنولوجيا

مجهول، موظف سابق شركة كبيرة للتكنولوجيا

مجهول، موظف سابق شركة كبيرة للتكنولوجيا

إدواردو بيرتوني،((Eduardo Bertonمركز الدراسات المعني بحرية التعبير والحصول على المعلومات (CELE)، الأرجنتين

دكتور هونج شيويه، (Hong Xue) أستاذ القانون مدير معهد سياسة الإنترنت والقانون، جامعة بيكين

مونيك فان جوى، (Monique Fanjoy) المسؤو ل الجديد للإعلام، مكتب مفوض الخصوصية، كندا

أبو بكر منير،((Abu Bakar Muni أستاذ القانون، كلية الحقوق، جامعة مالايا، ماليزيا

جوى مكناني (Joe McNamee)، منسق الدفاع بالاتحاد الأوربي، الحقوق الرقمية الأوربية

عمرو غربية، (Amr Gharbeia) المبادرة المصرية للحقوق الشخصية

جيمي هورسلي، (Jamie Horsle) باحث بارز ومحاضر في القانون، كلية ييل للقانون، نائب المدير، المركز الصيني للقانون

نيبوموسينو مالالاون (Nepomuceno Malaluan)، مدير مشارك، معهد حرية المعلومات، الفلبين

سينثيا، إم. ونغ. (Cynthia M. Wong) مدير، المشروع العالمي لحرية الإنترنت

سينفعه تونساراوس، (Sinfah Tunsarawuth)، محام وكاتب مستقل في الإعلام، بانكوك، تايلاند

بريم أوت فان دلان (Prim Ot van Daalen)، مدير، فتات الحرية، هولندا

سونيل أبراهام (Sunil Abraham)، مدير، مركز الإنترنت والمجتمع، الهند

الملحق 1:
الاختصارات

ACHPR	الميثاق الأفريقي لحقوق الإنسان والشعوب
ACHR	الاتفاقية الأمريكية لحقوق الإنسان
APEC	منتدى التعاون الاقتصادي لآسيا والمحيط الهادئ
CNIL	اللجنة الوطنية للمعلومات والحريات
COPPA	قانون حماية خصوصية الأطفال على الإنترنت
DPAI	الهيئة العامة لحماية البيانات في الهند
DPI	حزمة التفتيش العميق في الحزم
DSF	اتحاد الإشارات الرقمية
ECHR	الاتفاقية الأوروبية لحقوق الإنسان
ECPA	قانون خصوصية الاتصالات الالكترونية
EDRI	منظمة الحقوق الرقمية الأوروبية
EFF	مؤسسة Electronic Frontier Foundation
ENISA	وكالة أمن المعلومات والشبكات الأوروبية
EPIC	مركز معلومات الخصوصية الالكترونية
FRT	تقنية التعرف على الوجه
FTC	لجنة التجارة الاتحادية
GNI	مبادرة التجارة العالمية
GPS	أنظمة تحديد المواقع العالمية
GPS	أنظمة تحديد المواقع العالمية
ICCPR	العهد الدولي للحقوق المدنية والسياسية
IMEI	أدوات تعريف هوية الهاتف النقال الفريدة
IMF	صندوق النقد الدولي
IMSI	أدوات تعريف هوية بطاقة SIM
IP	بروتوكول إنترنت

ISP	مزود خدمات إنترنت
LLU	فصل الحلقات المحلية
MENA	منطقة الشرق الأوسط وشمال أفريقيا
MIIT	وزارة الصناعة وتكنولوجيا المعلومات
NAI	مبادرة شبكة الإعلانات
NTRA	الجهاز القومي لتنظيم الاتصالات
OAS	منظمة الدول الأمريكية
OECD	منظمة التعاون الاقتصادي والتنمية
OMB	مكتب الإدارة والموازنة
OSCE	منظمة الأمن والتعاون في أوروبا
OSP	مزود الخدمة من خلال الإنترنت
POPAI	بوينت أوف بيرشيس أدفيرتايزنج إنترناشونال
RFID	التعرف على الهوية بالترددات اللاسلكية
SAC	الإدارة الصينية للمقاييس
T&Cs	الشروط والأحكام
TRAI	هيئة تنظيم الاتصالات في الهند
UDHR	الإعلان العالمي لحقوق الإنسان

الملحق 2:
قائمة الأشكال والمربعات

تعمل منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو) ومن منطلق ما نص عليه نظامها الأساسي، على دعم «حرية تدفق الأفكار بالكلمات والصور»، ولقد آلت على نفسها العمل على تمكين فضاء الكتروني حر ومتاح يسهل للجميع الوصول إليه في إطار دعمها لحرية التعبير الشاملة على الانترنت وخارج الانترنت. ونأمل أن يكون هذا المنشور أداة مرجعية ذات فائدة لدول أعضاء اليونسكو والمعنيين الآخرين على المستوى القومي والمستوى الدولي، ونأمل أن يساهم في جمع المعنيين من أجل المناقشة المستنيرة حول المناهج المؤدية إلى حماية الخصوصية دون المساس بحرية التعبير. وفي السنوات القادمة، سوف تسعى اليونسكو خصيصاً إلى نشر معلومات تتعلق بالممارسات الجيدة والتعاون الدولي بشأن نقاط التداخل بين حرية التعبير والخصوصية. وسوف يظل البحث بشأن حماية مبدأ حرية التعبير في سياسة الإنترنت لمجموعة من المسائل جزءاً من الولاية الطبيعية لليونسكو والاستشارة الفنية التي تقدمها إلى المعنيين.

Jānis Kārkliņš

مدير عام مساعد قطاع الاتصالات والمعلومات، منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو)

توبي مندل، أندرو بوديفات، بن واجنر، ديكسي هوتن، نتاليا توريس

سلسلة اليونسكو بشأن حرية الانترنت
قطاع الاتصالات والمعلومات
منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو)

منشورات اليونسكو

حرية الاتصال
حرية التعبير
تغيير البيئة القانونية والتنظيمية الداعمة للإنترنت



قسم
الاتصال والمعلومات

منظمة الأمم المتحدة
للتربية والعلم والثقافة


9 789236 042411